ASCE STANDARD

ANSI/
ASCE/T&DI
21–05

Automated People Mover Standards—Part 1

Operating Environment
Safety Requirements
System Dependability
Automatic Train Control (ATC)
Audio and Visual Communications

This document uses both the International System of Units (SI) and customary units

ASCE

ANSI

T&DI
Transportation and Development Institute

ASCE STANDARD ANSI/ASCE/T&DI 21-05

American Society of Civil Engineers

Automated People Mover Standards—Part 1

This document uses both the International System of Units (SI) and customary units.

Operating Environment
Safety Requirements
System Dependability
Automatic Train Control (ATC)
Audio and Visual Communications

Published by the American Society of Civil Engineers

Library of Congress Cataloging-in-Publication Data

Automated people mover / American Society of Civil Engineers.
p. cm.
ISBN 0–7844–0873–4
1. Personal rapid transit. I. American Society of Civil Engineers.

TA1207.A95 2006
625.4—dc22 2006017165

Published by American Society of Civil Engineers
1801 Alexander Bell Drive
Reston, Virginia 20191
www.pubs.asce.org

ISBN 0–7844–0873–4
Manufactured in the United States of America.

STANDARDS

In 2003, the Board of Direction approved the revision to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by the Society. All such standards are developed by a consensus standards process managed by the Society's Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee made up of Society members and nonmembers, balloting by the membership of the Society as a whole, and balloting by the public. All standards are updated or reaffirmed by the same process at intervals not exceeding five years.

The following Standards have been issued:

ANSI/ASCE 1-82 N-725 Guideline for Design and Analysis of Nuclear Safety Related Earth Structures

ANSI/ASCE 2-91 Measurement of Oxygen Transfer in Clean Water

ANSI/ASCE 3-91 Standard for the Structural Design of Composite Slabs and ANSI/ASCE 9-91 Standard Practice for the Construction and Inspection of Composite Slabs

ASCE 4-98 Seismic Analysis of Safety-Related Nuclear Structures

Building Code Requirements for Masonry Structures (ACI 530-02/ASCE 5-02/TMS 402-02) and Specifications for Masonry Structures (ACI 530.1-02/ASCE 6-02/TMS 602-02)

ASCE/SEI 7-05 Minimum Design Loads for Buildings and Other Structures

SEI/ASCE 8-02 Standard Specification for the Design of Cold-Formed Stainless Steel Structural Members

ANSI/ASCE 9-91 listed with ASCE 3-91

ASCE 10-97 Design of Latticed Steel Transmission Structures

SEI/ASCE 11-99 Guideline for Structural Condition Assessment of Existing Buildings

ASCE/EWRI 12-05 Guideline for the Design of Urban Subsurface Drainage

ASCE/EWRI 13-05 Standard Guidelines for Installation of Urban Subsurface Drainage

ASCE/EWRI 14-05 Standard Guidelines for Operation and Maintenance of Urban Subsurface Drainage

ASCE 15-98 Standard Practice for Direct Design of Buried Precast Concrete Pipe Using Standard Installations (SIDD)

ASCE 16-95 Standard for Load Resistance Factor Design (LRFD) of Engineered Wood Construction

ASCE 17-96 Air-Supported Structures

ASCE 18-96 Standard Guidelines for In-Process Oxygen Transfer Testing

ASCE 19-96 Structural Applications of Steel Cables for Buildings

ASCE 20-96 Standard Guidelines for the Design and Installation of Pile Foundations

ANSI/ASCE/T&DI 21-05 Automated People Mover Standards—Part 1

ASCE 21-98 Automated People Mover Standards—Part 2

ANSI/ASCE 21-00 Automated People Mover Standards—Part 3

SEI/ASCE 23-97 Specification for Structural Steel Beams with Web Openings

ASCE/SEI 24-05 Flood Resistant Design and Construction

ASCE/SEI 25-06 Earthquake-Actuated Automatic Gas Shutoff Devices

ASCE 26-97 Standard Practice for Design of Buried Precast Concrete Box Sections

ASCE 27-00 Standard Practice for Direct Design of Precast Concrete Pipe for Jacking in Trenchless Construction

ASCE 28-00 Standard Practice for Direct Design of Precast Concrete Box Sections for Jacking in Trenchless Construction

SEI/ASCE/SFPE 29-99 Standard Calculation Methods for Structural Fire Protection

SEI/ASCE 30-00 Guideline for Condition Assessment of the Building Envelope

SEI/ASCE 31-03 Seismic Evaluation of Existing Buildings

SEI/ASCE 32-01 Design and Construction of Frost-Protected Shallow Foundations

EWRI/ASCE 33-01 Comprehensive Transboundary International Water Quality Management Agreement

EWRI/ASCE 34-01 Standard Guidelines for Artificial Recharge of Ground Water

EWRI/ASCE 35-01 Guidelines for Quality Assurance of Installed Fine-Pore Aeration Equipment

CI/ASCE 36-01 Standard Construction Guidelines for Microtunneling

SEI/ASCE 37-02 Design Loads on Structures During Construction

CI/ASCE 38-02 Standard Guideline for the Collection and Depiction of Existing Subsurface Utility Data

EWRI/ASCE 39-03 Standard Practice for the Design and Operation of Hail Suppression Projects

ASCE/EWRI 40-03 Regulated Riparian Model Water Code
ASCE/EWRI 42-04 Standard Practice for the Design and Operation of Precipitation Enhancement Projects
ASCE/SEI 43-05 Seismic Design Criteria for Structures, Systems, and Components in Nuclear Facilities
ASCE/EWRI 44-05 Standard Practice for the Design and Operation of Supercooled Fog Dispersal Projects
ASCE/EWRI 45-05 Standard Guidelines for the Design of Urban Stormwater Systems
ASCE/EWRI 46-05 Standard Guidelines for the Installation of Urban Stormwater Systems
ASCE/EWRI 47-05 Standard Guidelines for the Operation and Maintenance of Urban Stormwater Systems

CONTENTS

FOREWORD

In 2003, the Board of Direction approved the revision to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by the Society. All such standards are developed by a consensus standards process managed by the Society's Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee made up of Society members and nonmembers, balloting by the membership of the Society as a whole, and balloting by the public. All standards are updated or reaffirmed by the same process at intervals not exceeding five years.

This standard was developed for Automated People Movers.

An Automated People Mover (APM) is defined as a guided transit mode with fully automated operation, featuring vehicles that operate on guideways with exclusive right-of-way.

This standard has been prepared by the ASCE Automated People Mover Standards Committee. It establishes the minimum set of requirements necessary to achieve an acceptable level of safety and performance for an APM system. As such, it may be used in the safety certification process. The overall goal of this standard is to assist the industry and the public by establishing standards for APM systems.

This standard includes minimum requirements for the design, construction, operation, and maintenance of APM systems.

This standard has no legal authority in its own right but may acquire legal standing in one or more of the following ways:

1. Adoption by an authority having jurisdiction
2. Reference to compliance with the standard as a contract requirement
3. Claim by a manufacturer or manufacturer's agent of compliance with the standard

This standard has been prepared in accordance with recognized engineering principles and should not be used without the user's competent knowledge for a given application. The publication of this standard by ASCE is not intended as warrant that the information contained therein is suitable for any general or specific use, and the Society takes no position respecting the validity of patent rights. The user is advised that the determination of patent rights or risk of infringement is entirely their own responsibility.

This page intentionally left blank

ACKNOWLEDGMENTS

The American Society of Civil Engineers (ASCE) acknowledges the devoted efforts of the Automated People Mover Standards Committee under the Lifeline Standards Council of the Codes and Standards Committee. This group comprises individuals from many backgrounds including: consulting engineering, research, transit agencies, airports, transit system design and manufacturing, education, government, and private practice.

This standard was prepared through the consensus standards process by balloting in compliance with procedures of ASCE's Codes and Standards Activity Council. Those individuals who serve on the Automated People Mover Standards Committee are:

Thomas J. McGean, Chair*
Tedd L. Snyder, Vice-Chair*
Lawrence L. Smith, Secretary*
Joseph D. Abbas
Douglas T. Baird
Frank P. Bares
Cheryl Boehm
Murthy V. A. Bondada
Jon Brackpool
Pierre A. Brunet
David B. Campbell
John J. Champ
Yves Clarissou
Redjean Clerc
Frank Culver
Peter DeLeonardis
John Dexter
Paul Didrikson
Didier Dupre
Charles P. Elms
Robert W. Falvey
Jimmy E. Fletcher
Matthias Frenz
Henri Frey
Darin Friedmann
Antonio Garcia
Franklin D. Gates
Robert R. Griebenow
Greg B. Hale
Albert W. Hartkorn
William T. Hathaway
James Hoelscher
Gary W. Houts
Victor Howe
Alex R. Inserto
James Mike Johnson
John Kapala
Ronald D. Kangas*
Alexander Klimmer
J. Sam Lott
Martin V. Lowson
Stanford W. Lynch
Charles Martin
Diane I. Morse
Jorg Nahke
Josef Nejez
Hiroshi Ogawa
Richard R. Prell
Felix Rhyner
Michael R. Riseborough
William Rourke
Obe Schrader
William P. Showalter
Michael Shumack
David Taliaferro
David Thurston
James M. Tuten
Michael S. Venter
Gert Vestergaard
Rudiger Vom Hovel
Thomas Waldron
Ray Warner
Lloyd J. Welch
Steven K. Yates

* Committee Control Group Members

The following Working Group Leaders are especially acknowledged for their efforts in drafting specific sections of the standard and shepherding them through the consensus process.

General: Michael Shumack
Operating Environment: Drafting: Maury Sulkin; Reaffirmation: John Dexter
Safety Requirements: Drafting: James Hoelscher with Ronald Kangas, William Hathaway, and Charles Martin; Reaffirmation: Jim Hoelscher et al.
System Dependability: Drafting: J. Sam Lott; Reaffirmation: Joe Abbas
Automatic Train Control: Drafting: Charles Martin with Robert Good; Reaffirmation: Charles Martin with Jim Hoelscher and Al Hartkorn
Audio and Visual Communications: Drafting: Charles Elms; Reaffirmation: Charles Elms with Paul Didrickson.

ASCE Staff support was provided by John Esslinger. Michael Shumack provided Configuration Control. Support for our membership mailings and communication was Frank Culver and Lawrence Smith. Website was provided by Atlanta Hartsfield International Airport and Michael Shumack. Support for meetings was provided by BAA, United Kingdom; Bombardier, Inc.; Clark County, Nevada; Denver International Airport; Doppelmayr Cable Car GmbH & Co.; Horton Automatics; McCarran International Airport; Miami-Dade Transit; Washington Group International; and Walt Disney Enterprises.

Automated People Mover Standards—Part 1

1.0 GENERAL

1.1 SCOPE

This standard has been divided into four parts to expedite the approval and release process as well as to facilitate ease of use. This document constitutes Part 1 of the Standard.

Parts 1, 2 and 3 cover a minimum set of requirements for design of an automated people mover (APM) with an acceptable level of safety and performance.

Part 1 consists of:

1. General
2. Operating Environment
3. Safety Requirements
4. System Dependability
5. Automatic Train Control (ATC)
6. Audio and Visual Communications

Part 2 consists of:

1. General
7. Vehicles
8. Propulsion and Braking

Part 3 consists of:

1. General
9. Electrical
10. Stations
11. Guideways

Part 4 is a minimum set of requirements for maintaining an acceptable level of safety and performance for an APM in passenger operation.

Part 4 consists of:

12. Security
13. Emergency Preparedness
14. System Verification and Demonstration
15. Operations, Maintenance, and Training
16. Operational Monitoring

1.2 EXISTING APPLICATIONS

Existing installations and projects in progress prior to the effective date of this standard need not comply with the new or revised requirements of this edition, except where specifically required by the authority having jurisdiction. Existing APMs, when completely removed and reinstalled, shall be classified as new installations.

1.3 NEW APPLICATIONS

New installations begun after the effective date of this standard shall comply with the new or revised requirements of this edition.

1.4 REFERENCE STANDARDS

The following documents or portions thereof are incorporated by reference in this Standard.

ANSI Publications: American National Standards Institute, Attn: Customer Service, 11 West 42nd Street, New York, NY 10036, phone (212) 642-4900.

ANSI S1.4–1983, *Specification for sound level meters* (cited in Section 2.2.1)

ANSI S3.29–1983, *Guide to the evaluation of human exposure to vibration in buildings* (cited in Section 2.2.2)

IEEE Publications: The Institute of Electrical and Electronic Engineers, 3 Park Avenue, New York, NY 10016-5997, phone (800) 678-4333.

IEEE Std 1474.1–2004, IEEE *standard for communications-based train control (CBTC) performance and functional requirements* (cited in Section 5.0)

NFPA Publication: National Fire Protection Association, Customer Service Department, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101, phone (800) 344-3555

NFPA 72–2002 *National fire alarm code* (cited in Section 6.1.6)

NFPA 130–2003 *Standard for fixed guideway transit and passenger rail systems* (cited in Section 6.1.2)

UL Publication: Underwriters Laboratories, Publications, 333 Pfingsten Road, Northbrook, IL 60062, phone (847) 272-8800

UL96A–11th edition, 2001, *Installation requirements for lightning protection systems* (cited in Section 2.1.4)

UL 813–1993– *Commercial audio equipment* (cited in Section 6.1.3)

Telecommunications Industry Association Publication: Telecommunications Industry Association, 2500 Wilson Blvd., Suite 300, Arlington VA 22201, phone (703) 907-7700

TIA/EIA Telecommunications Systems Bulletin TSB-88-A-1, January 2002, *Wireless communications systems–performance in noise and interference–limited situations–recommended methods for technology–independent modeling, simulation and verification–addendum 1* (cited in Section 6.1.6)

Code of Federal Regulations: U.S. Government Printing Office, Superintendent of Documents, 732

North Capitol Street, N.W., Washington, DC 20401, phone (202) 512-1800

CFR, Title 47, Chapter I, Part 15, *Radio frequency devices* (cited in Section 2.2.3)
CFR, Title 47, Chapter I, Part 90, Subparts S and T, *Private land mobile radio services* (cited in Section 2.2.3)

Military Standards: Defense Printing Service, Building A, 700 Robbins Avenue, Philadelphia, PA 19111, phone (215) 697-2179 or 2667

MIL-STD-461E, *Requirements for the control of electromagnetic emissions and susceptibility* (cited in Section 2.1.8)
MIL-STD-810 F, *Environmental test methods and engineering guidelines* (cited in Section 2.1.5)

NOAA Publication: National Climatic Data Center, 151 Patton Ave., Room 120, Ashland, NC 28801-0900, phone (828) 271-4800

National Oceanic and Atmospheric Administration, *Local climatologic data, annual summary with comparative data,* updated annually (cited in Section 2.1)

Gale Research Publication: Gale Research Company, P.O. Box 33477, Detroit, MI 48232, phone (800) 877-4253, Ext. 5477

Richard A. Wood, Ph.D. *Weather of U.S. cities,* Fifth Edition, Vols. 1 and 2, 1996 (cited in Section 2.1)

1.5 DEFINITIONS

Automated People Mover (APM): A guided transit mode with fully automated operation, featuring vehicles that operate on guideways with exclusive right-of-way.

Automatic Train Control (ATC): The system for automatically controlling train movement, enforcing train safety, and directing train operations. ATC includes subsystems for automatic train operation (ATO), automatic train protection (ATP) and automatic train supervision (ATS).

Automatic Train Operation (ATO): The subsystem within the automatic train control system that performs any or all of the functions of speed regulation, programmed stopping, door and dwell-time control, and other functions otherwise assigned to the train operator.

Automatic Train Protection (ATP): The subsystem within the automatic train control system that provides the primary protection for passengers, personnel, and equipment against the hazards of operations conducted under automatic control.

Automatic Train Supervision (ATS): The subsystem within the automatic train control system that monitors and manages the overall operation of the APM system and provides the interface between the system and the central control operator.

Braking, Emergency: Irrevocable braking to a complete stop at a rate never less than the minimum guaranteed rate.

Braking, Service: Braking of vehicle motion at a rate that is regarded as comfortable for repeated use in service stopping and/or slowing.

Central Control: The location where automatic train supervision is accomplished for the entire transit system; the train command center.

Central Control Operator: Any person authorized to operate the APM system from Central Control.

Consist: The makeup or composition (number and specific identity) of a train of vehicles.

Dwell Time: The total time the train services the station measured as the time from door open command to the time the doors are closed and locked.

Dynamic Sign: A sign on which the messages can be changed.

Fail-Safe: A characteristic of a system or its elements whereby any failure or malfunction affecting safety will cause the system to revert to a state that is known to be safe.

Failure: An inability to perform an intended function.

Free Field: An isotropic, homogeneous sound field that is free from all bounding surfaces.

Hazard: An existing or potential condition that can result in an accident.

Headway: The time separation between two trains, both traveling in the same direction on the same guideway, measured from the time the head end of the leading train passes a given reference point to the time the head end of the train immediately following passes the same reference point.

Interlock: An arrangement of control elements so interconnected that their operations must succeed each other in proper sequence.

Jerk: The time rate of change of acceleration or deceleration.

MTBHE: Mean time between hazardous events.

Overspeed: Train speed that is in excess of the speed limit as defined for the relevant point on the guideway.

Overtravel: Continued movement of a train beyond a specified stopping point.

Passenger Compartment: If a vehicle is divided into separate areas between which passengers are either unable or not permitted to move, each such area is defined as a passenger compartment. If the vehicle is

not so divided, then the entire vehicle is the passenger compartment.

Permissive Decision: Granting permission or authority for the system or a part of the system to enter any state other than the safe state.

Risk: A measure of the severity and likelihood of an accident.

Safe State: System state that is deemed acceptable by the hazard resolution process (see Section 3.1.2).

Safety Critical: A designation placed on a system, subsystem, element, component, device, or function denoting the satisfactory operation of which is mandatory to mitigation of unacceptable and undesirable hazards as defined in Section 3.4, Table 3-1.

Separation: The distance between the adjacent ends of two trains traveling along the same guideway as measured along the guideway centerline.

Shall: In this standard, the word "shall" denotes a mandatory requirement.

Should: In this standard, the word "should" denotes a recommendation.

Subsystem: A major functional subassembly or grouping of items or equipment that is essential to operational completeness of a system.

System: A composite of people, procedures, facilities, and/or equipment that are integrated to perform a specific operational task or function within a specific environment.

System Dependability: The overall set of criteria used to measure the performance of an operating system in terms of reliability, maintainability, and availability.

System Safety: The application of engineering and management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

Train: A consist of one or more contiguous vehicles combined into an operating unit.

Vehicle: The smallest unit that can operate alone or that comprises one of the basic building blocks of a train.

Zero Speed: A specified speed below which Automatic Train Control considers a train to be stopped.

2.0 OPERATING ENVIRONMENT

There are two aspects to operating environment considerations. One deals with the existing environmental conditions in which the system must operate (ambient) and the other deals with the environment resulting from the existence and operation of the system (induced). Both of these aspects are covered herein.

2.1 AMBIENT CONDITIONS

One of the following two sources of historical climatic data shall be considered when specifying design climatic values: Source Number 1 is a basic compilation of low, high, and mean values of temperature, humidity, steady and gusting winds, rainfall rates, and other climatic characteristics as compiled by the National Oceanic & Atmospheric Administration (NOAA). Source Number 2 summarizes the NOAA data in convenient form.

1. *Local climatologic data, annual summary with comparative data, national oceanic and atmospheric administration,* updated annually.
2. *Weather of U.S. cities,* Fifth Edition, Volumes 1 and 2, Richard A. Wood, PhD, Gale Research Company, Detroit, Michigan, 1996; Library of Congress Card Number 87–11869, ISBN 0–8103–5525–6.

Where the proposed site is located outside of the area of coverage of the above documents, or within a microclimate, appropriate local weather data shall be used in lieu of the above sources.

2.1.1 Temperature and Humidity

The system shall be designed to, and capable of operating in, site temperature conditions that represent the 50-year highest and lowest temperature of record and at a noncondensing relative humidity of 95% at a temperature of 30 °C (86 °F).

2.1.2 Wind

Maximum wind speeds shall be established for at least the following conditions:

1. Normal system operation
2. Manual operation
3. System survival

The maximum wind speed for normal system operation shall be used as the design wind speed for safe automated system operation. If this wind speed is exceeded, automated operation shall not be permitted or shall be appropriately degraded.

The maximum wind speed for manual system operation shall be used as the design wind speed for safe manual operation. If this wind speed is exceeded, the system shall not be permitted to operate.

The maximum wind speed for system survival shall be the design wind speed for all structures. This wind speed shall be that used by local building codes.

2.1.3 Precipitation

If the system is intended for operation while subjected to rainfall, snowfall, and icing, it shall be designed for operation at rates consistent with historical data.

2.1.4 Lightning

Protection shall be provided against lightning incidence in the area for those systems that are susceptible. Such protection should be in compliance with *Installation requirements for lightning protection systems,* UL96A, 11th edition, 2001.

2.1.5 Existing Atmospheric Pollution

The system design shall tolerate atmospheric pollutants that exist at the site. Such pollutants may include dust, dirt, salt, ozone, smog, and other matter specific to the site. In the cases of dust and dirt, compliance shall be with *Environmental test methods and engineering guidelines,* MIL-STD-810 F, method 510.4.

2.1.6 Solar Heat Load

The design of systems that are subject to solar heating shall be based on a peak, direct solar heat gain appropriate to the site. Material selection shall minimize the deleterious effects of ultraviolet radiation.

2.1.7 Flood Zones

Flood levels shall be specified as the 100-year flood level. The system shall be capable of surviving flooding with minimal damage to structure and equipment. Equipment and facility elements that can be damaged by flooding shall be protected or installed above the flood plain elevation.

2.1.8 Electromagnetic Background

The system and all of its components shall be electromagnetically compatible with the site environment at the initiation of system operation. All system electrical and electronic equipment shall function satisfactorily in the presence of electromagnetic emissions generated externally at the site. The environment may include, but is not limited to: communications systems, microwave facilities and transmissions, television and radio transmitters and repeaters, radar systems, computer equipment and accessories, traffic control devices, magnetometers, electric motors, controls, power tools, welders, x-ray equipment, power substations and equipment, automotive vehicles, aircraft, and high voltage power lines. The electromagnetic environment particular to the site should be determined and the design should provide for elimination of the influence of these conditions upon the equipment. Compliance shall be in accordance with *Requirements for the control of electromagnetic emission and susceptibility,* MIL-STD-461E, Requirement Matrix category "Ground, Army."

2.2 INDUCED ENVIRONMENTAL PARAMETERS

The system shall be operated, stored, and maintained without imposing on the site any condition that exceeds the limitations defined herein.

2.2.1 Exterior Airborne Noise

The following exterior noise levels emanating from the system with all equipment operating normally should not be exceeded under the conditions defined. Exterior noise levels shall be measured using at least a Type II instrument, as defined in *Specification for sound level meters,* ANSI Standard S1.4–1983, and shall be set for fast or slow response as indicated.

1. Vehicle entering/leaving a station—inside station, 1.5m (5 feet) from platform edge and 1.5m (5 feet) above platform surface: 76 dBA (slow response).
2. Vehicle stopped in station—inside station, 1.5m (5 feet) from platform edge and 1.5m (5 feet) above platform surface: 74 dBA (slow response). Vehicle doors and platform doors (if provided) shall be fully open.
3. Under all normal operating conditions in a free field, 15m (50 feet) from guideway centerline and from 1.5m (5 feet) above ground level to 1.5m (5 feet) above guideway running surface: 76 dBA (fast response).

Noticeable pure tones are not permitted. A pure tone is defined to exist when one 1/3-octave band exceeds the arithmetic average of the two adjacent bands by 4 dBA or more in the range of frequencies between 250 and 8,000 Hz. If an adjacent band contains a pure tone, the next closest band without a pure tone shall be used in its place. A noticeable pure tone shall be considered to exist when the 1/3-octave band containing the pure tone contributes more than 1.0 dBA to the overall dBA level.

More stringent noise requirements may be necessary to satisfy local environmental limitations.

2.2.2 Structure-Borne Noise/Vibration

System-induced vibrations shall be imperceptible at or in surrounding buildings. The threshold of perception shall be as defined by *Guide to the evaluation of human exposure to vibration in buildings,* ANSI Standard S3.29–1983.

2.2.3 Electromagnetic Radiation

The system shall be electromagnetically compatible with its environment. The system shall not produce electromagnetic emissions, whether conducted, radiated, or induced, that interfere with normal operation of electromagnetic devices or equipment used in and around the site at the initiation of system operation.

All system transmitting and receiving equipment, such as for automatic train control (ATC) and audio and visual communications, shall meet the licensing requirements of the Code of Federal Regulations, Title 47, Chapter I, Part 90, *Private Land Mobile*

Radio Services, Subparts S and T; and the interference requirements defined in Title 47, Chapter I, Part 15, *Radio Frequency Devices.*

3.0 SAFETY REQUIREMENTS

A System Safety Program, per Section 3.1, shall be instituted during the system planning/design phase and continue throughout the system construction and operation. The system safety concept shall emphasize the prevention of accidents by resolving hazards in a systematic manner in accordance with Section 3.1.2, *Hazard Resolution Process.*

3.1 SYSTEM SAFETY PROGRAM

A System Safety Program shall be implemented to identify and resolve hazards. The owner shall provide for the development of a System Safety Program Plan to assist in implementing and documenting that program. The System Safety Program Plan shall identify the responsibilities of all parties for implementing a System Safety Program.

The System Safety Program and Plan shall:

1. Have as their objective to provide for the safety of the passengers, employees, general public, and equipment
2. Encompass all system elements and organizations within the automated people mover (APM) system
3. Identify the safety roles and responsibilities of all organizational elements, and require accountability
4. Designate one individual to be responsible for the safety of the system who has a clearly defined role and responsibilities established through a written policy
5. Contain a hazard resolution process that includes the procedures necessary to identify and resolve hazards throughout the system life cycle
6. Provide for and maintain owner/management commitment in the form of an adopted policy and the allocation of resources

The individual identified to carry out the System Safety Program shall have clear evidence of the authority to insure its implementation and shall report directly to top management.

3.1.1 System Safety Program Plan

A System Safety Program Plan (SSPP) shall be developed during the planning/design phase of the APM project and maintained current throughout the APM system life cycle. The SSPP shall be prepared in general accordance with Annex A, *System Safety Program Requirements,* A.1 (*System Safety Program Plan*), or equivalent. The SSPP shall, as a minimum, identify the scope of the *System Safety Program* activities including those identified in Section 3.1.

3.1.2 Hazard Resolution Process

The hazard resolution process shall be initiated by defining the physical and functional characteristics of the APM system to be analyzed. These characteristics shall be presented in terms of the major elements that make up the system and its environment, including equipment, facilities, procedures, and people.

The hazards shall be identified. The techniques and methods used to identify the hazards shall include:

1. Data from previous accidents or operating experience
2. Expert opinion and hazard scenarios
3. Checklists of potential hazards
4. Previous hazard analyses
5. Other analysis techniques as appropriate

All identified hazards shall be assessed in terms of the severity or consequence of the hazard and the probability of occurrence.

Risk assessment estimates (Section 3.4, Table 3-1) shall be used as the basis in the decision-making process to determine whether individual APM system or subsystem hazards shall be eliminated, mitigated, or accepted. Hazards shall be resolved through a design process that emphasizes the elimination of the hazard. Resolution strategies or countermeasures to be employed, listed in order of decreasing preference, shall be the following:

1. Design to eliminate hazards
2. Design to control hazards
3. Use safety devices
4. Use warning devices
5. Implement special procedures
6. Accept the hazard
7. Eliminate the system/subsystem/equipment

This process shall include full documentation of the hazard resolution activities. The effectiveness of the countermeasures shall be monitored to determine that no new hazards are introduced. In addition, whenever substantive changes are made to the system, analyses shall be conducted to identify and resolve any new hazards.

3.1.2.1 Hazard Analyses

Hazard analyses shall be employed to assist in the evaluation of potential hazards and to document their resolution. As a minimum, a Preliminary Hazard Analysis (PHA) shall be conducted for each new APM system project. Other detailed analyses including Subsystem Hazard Analysis (SSHA), System Hazard

Analysis (SHA) and Operating and Support Hazard Analysis (O&SHA) shall also be conducted if mandated by the SSPP. These analyses shall be conducted in general accordance with Annex A, *System Safety Program Requirements,* sections A.2 (PHA), A.3 (SSHA), A.4 (SHA), and A.5 (O&SHA), or equivalent, respectively.

3.2 SAFETY PRINCIPLES

The following safety principles shall be observed in the APM system (see Section 3.4, Table 3-1, for the definition of unacceptable and undesirable hazards):

1. When the system is operating normally there shall be no unacceptable or undesirable hazard conditions.
2. The system design shall require positive actions to be taken in a prescribed manner to either begin system operation or continue system operation.
3. The safety of the system in the normal automatic operating mode shall not depend on the correctness of actions or procedures used by operating personnel.
4. There shall be no single-point failures in the system that can result in an unacceptable or undesirable hazard condition.
5. If one failure combined with a second failure can cause an unacceptable or undesirable hazard condition, the first failure shall be detected before the second failure occurs.
6. Software faults shall not cause an unacceptable or undesirable hazard condition.
7. Unacceptable hazards shall be eliminated by design.
8. Maintenance activities required to preserve risk levels (Section 3.4, Table 3-1) shall be prescribed to the individual responsible for the *System Safety Program* (Section 3.1) during the design phase. These maintenance activities shall be minimized in both the frequency and in the complexity of their implementation. The personnel qualifications required to adequately implement these activities shall also be identified.

3.3 AUTOMATIC TRAIN CONTROL SYSTEM FAIL-SAFE DESIGN

All safety critical elements of the automatic train control (ATC) system (see Section 5.0, *Automatic Train Control*) shall be designed and implemented in accordance with fail-safe principles and shall use one or more of the techniques described below, or equivalent, to detect potentially unsafe failure modes and force the system to a known safe state. Fail-safe principles shall be realized by designing the system to have intrinsically safe failure characteristics or by designing the system with verifiable techniques that detect potentially unsafe failures and ensure that the system reverts to a known safe state. Documentation of the means used and proof that the fail-safe principle has been met shall be required for every safety critical system or subsystem.

3.3.1 Intrinsic Fail-Safe Design

Intrinsically fail-safe systems shall be designed using verifiable physical, mechanical, and/or electrical component characteristics. For these designs, the effect of every relevant failure mode on the operation of the system shall be considered, analyzed, and documented in a comprehensive failure modes and effects analysis, or equivalent.

3.3.2 Alternatives to Intrinsic Fail-Safe Design

Many control system designs utilize integrated circuits, microprocessors, and software to achieve the required functional characteristics. Designs that do not exhibit intrinsically safe failure characteristics shall use one or more of the following techniques (Section 3.3.2.1 through Section 3.3.2.4). The effectiveness and completeness of these techniques shall be documented and proven as part of system *Validation and Verification* (Section 3.4). The measure of the technique's effectiveness shall assess its ability to detect fault conditions and assure that the technique is installed as designed and is required for the system to operate.

3.3.2.1 Checked-Redundancy

The application of the checked-redundant principle shall include at least two parallel systems performing identical functions. A means shall be provided to compare the output of the parallel systems. If the two systems do not agree, then the safety critical function being performed shall default to a known safe state. The following characteristics shall be incorporated and verified in the checked-redundant design:

1. The checking process shall assure that "agreement" shall not be indicated unless the redundant outputs agree. Lack of "agreement" of the checking process shall result in a known safe state.
2. The checking process shall include the comparison of all safety critical results of all the safety critical functions.
3. Any failure that could affect system safety in either of the redundant units shall result in a known safe state.
4. The redundant units shall be independent from each other so that no common environmental or power fluctuations, errors, and/or faults can cause unacceptable or undesirable hazards (Section 3.4, Table 3-1).
5. The checking process shall be comprehensive in coverage (functions tested and the rate at which functions are tested) to ensure that the probability of

failures or compensating failures producing unacceptable or undesirable hazards is at an acceptable level (Section 3.4, Table 3-1).
6. For units employing software-programmed elements, the software shall be shown to be free from errors including any errors introduced during the compilation process by proven principles/practices of verification and validation (Section 3.4).

3.3.2.2 N-Version Programming

The application of the N-version programming principle shall require at least two parallel programmed systems performing identical functions. The software in each system shall be unique and independently written by different persons/teams, using different languages and tools. The hardware may or may not be identical, or may include both programmed systems within one hardware processing unit. A means shall be provided to compare the output of the parallel programmed systems. If the two systems do not agree, then the safety critical function being performed shall default to a known safe state. The following characteristics shall be incorporated and verified in the design:

1. The checking process shall be fail-safe. "Agreement" shall not be indicated unless the redundant outputs agree. Lack of "agreement" of the checking process shall result in a known safe state.
2. The checking process shall include the comparison of all safety critical results of all the safety critical functions.
3. Any failure that could affect system safety in either of the units shall result in a known safe state.
4. The parallel programmed systems shall be independent from each other so that no common environmental or power fluctuations, errors, and/or faults can cause unacceptable or undesirable hazards (Section 3.4, Table 3-1).
5. The checking process shall be comprehensive in coverage (functions tested and the rate at which functions are tested) to ensure that the probability of failures or compensating failures producing unacceptable or undesirable hazards is at an acceptable level (Section 3.4, Table 3-1).
6. The software processed by the parallel programmed systems shall be proven to be independent.

3.3.2.3 Diversity and Self-Checking

The use of diversity and self-checking concepts shall require that all critical functions be performed in diverse ways, using diverse software operations and/or diverse hardware channels, and that critical system hardware be tested with self-checking routines. Permissive outputs shall be allowed only if the results of the diverse operations correspond and the self-checks reveal no failures. The following characteristics shall be incorporated and verified in the design:

1. The checking of the results of the diverse operations shall be fail-safe. Permissive decisions shall not be allowed unless the diverse results agree. Lack of "agreement" of the diverse checking process or of self-checks shall result in a known safe state.
2. The diverse operations and the self-checking process shall include the verification of all safety critical results of all the safety critical functions.
3. Any failure that could affect system safety shall result in a known safe state.
4. The diversity and self-checking routines shall be comprehensive in coverage (functions tested and rate at which functions are tested) to ensure that the probability of failures or compensating failures producing unacceptable or undesirable hazards is at an acceptable level (Section 3.4, Table 3-1).
5. For units employing software-programmed elements, the software shall be shown to be free from errors including any errors introduced by the compilation process by proven principles/practices of *Verification and Validation* (Section 3.4).

3.3.2.4 Numerical Assurance

The numerical assurance principle shall require permissive decisions to be represented by large unique numerical values, calculated by combining numerical values representing each of the critical constituents of a permissive decision. The following characteristics shall be incorporated and verified in the design:

1. The numerical values representing the permissive decisions shall be proven to be unique and to require unique values added by each of the critical constituents.
2. All critical processes that do not add unique values to the permissive results, per (1), shall generate unique numerical values that are verified for correctness.
3. The system calculating the numerical results must have no prior knowledge of the correct permissive numerical values.
4. The process used to verify the correctness of the numerical results shall be fail-safe.
5. Any failure that could affect system safety shall result in a known safe state.
6. Lack of correctness of any of the numerical results shall result in a known safe state.
7. The numerical process shall be comprehensive in coverage (functions protected by numerical values

and the frequency at which the numerical values are calculated and verified) to ensure that the probability of failures or compensating failures producing unacceptable or undesirable hazards is at an acceptable level as defined in Section 3.4, Table 3-1.

3.4 VERIFICATION AND VALIDATION

The design and implementation of all safety critical hardware and software elements of the system as identified in the *Hazard Resolution Process* (Section 3.1.2) shall be subjected to verification and validation. This includes elements designed and implemented in accordance with *Safety Principles* (Section 3.2) and *Automatic Train Control System Fail-Safe Design* (Section 3.3). The objective of this verification and validation shall be to verify that all safety critical elements have been designed and implemented to achieve safe operation and to verify the level of safety achieved.

The verification and validation process shall include:

1. The identification of all factors upon which the assurance of safety depends. Such factors shall be directly associated with the design concept used, For example, *Checked-Redundancy, N-Version Programming, Diversity* and *Self-Checking,* or *Numerical Assurance.*
2. The identification of all safety critical functions performed by the system.
3. Analyses demonstrating that all dependent factors have been satisfied and that each safety critical function has been implemented in accordance with safety principles.

The ATC system (see Section 5.0, *Automatic Train Control*) shall, in addition to the above, have a calculated aggregate MTBHE (total of all catastrophic and critical hazards) of 10**8 (10 × E 8) system operating hours or greater. System safety documentation shall support this aggregate MTBHE calculation and substantiate the methodology used to arrive at the result.

4.0 SYSTEM DEPENDABILITY

System Dependability is the overall set of criteria used to measure the performance of an operating system in terms of reliability, maintainability, and availability. It shall be established in accordance with the principles outlined in this section.

TABLE 3-1. Risk Assessment

Frequency of occurrence	Hazard Severity			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A—Frequent	IA	IIA	IIIA	IVA
B—Probable	IB	IIB	IIIB	IVB
C—Occasional	IC	IIC	IIIC	IVC
D—Remote	ID	IID	IIID	IVD
E—Improbable	IE	IIE	IIIE	IVE

IA, IIA, IIIA, IB, IIB, & IC = Unacceptable.
IIIB, IIC, & ID = Undesirable (allowable with agreement from authority having jurisdiction).
IVA, IVB, IIIC, IID, IIID, IE, & IIE = Acceptable with notification to the authority having jurisdiction.
IIIE, IVC, IVD, & IVE = Acceptable.

A—Frequent = MTBHE is less than 1,000 operating hours.
B—Probable = MTBHE is equal to or greater than 1,000 operating hours and less than 100,000 operating hours.
C—Occasional = MTBHE is equal to or greater than 100,000 operating hours and less than 1,000,000 operating hours.
D—Remote = MTBHE is equal to or greater than 1,000,000 operating hours and less than 100,000,000 operating hours.
E—Improbable = MTBHE is equal to or greater than 100,000,000 operating hours.

It is understood that the quantification of the probability or frequency of occurrence of elements within the safety verification process may be required to be subjectively (i.e., qualitatively) determined. All subjectivelly determined elements shall be identified, and the rationale and justification for the estimation shall be described.

I—Catastrophic = Death, system loss, or severe environmental damage.
II—Critical = Severe injury, severe occupational illness, or major system or environmental damage.
III—Marginal = Minor injury, minor occupational illness, or minor system or environmental damage.
IV—Negligible = Less than minor injury, occupational illness, or less than minor system or environmental damage.

Throughout this section, references to "system" may also be applied to "system subsets" for purposes of determining their individual contribution to the overall System Dependability.

Partial service or degraded service adjustments may be applied in defining overall System Dependability. The use of factors, or ratios, or of separate calculations by system subset may be used to provide for such adjustments.

4.1 SERVICE RELIABILITY

Service reliability is defined as the mean time between system or system subset failure ($MTBF_s$).

$$MTBF_s = \frac{\text{Operating Hours}}{\text{Number of Failures}} = OH_s / NF_s$$

where:

OH_s = Total number of hours of scheduled operation over which the service reliability is being determined; the Period of Operating Hours

NF_s = Number of failures, malfunctions, and operating disruptions classified as service interruptions during the Period of Operating Hours, OH_s

4.1.1 Service Interruptions

Service interruptions are those events or failures that prevent passenger use of the system or system subset as intended. Service interruptions shall be defined and weighted in accordance with their relative importance. At a minimum, the following types of service interruptions shall be included:

1. Unscheduled stoppage of one or more trains.
2. Rerouting of trains due to equipment malfunction so that any stations normally served are not served.
3. Door malfunctions that prevent passengers from entering or exiting trains at stations in automatic operation.
4. Malfunctions that result in potentially hazardous operations.

The owner will specify if erroneous operator actions that result in service interruptions are to be included.

4.1.2 Exceptions

The following shall not be considered service interruptions:

1. Malfunctions that result in an interruption of normal train operations for an interval of time equal to or less than a specified period of time (Grace Time).
2. Malfunctions or disruptions due to vandalism, passenger misuse of the system, or passenger-induced delays.
3. Disruptions caused by unauthorized intrusion of persons, animals, or inanimate objects into the system, except where the intrusion or failure results from the malfunction of any security system or devices designed to protect against such intrusion.
4. Disruptions due to external causes, including loss of primary power, police or security directives, force majeure, or environmental conditions beyond specified limits.
5. Disruptions for special training, guideway inspections, or extended repair purposes that have been arranged in advance.
6. Stoppages due to normal functioning of the automatic train control system where specified operating performance requirements are met.

4.2 SERVICE MAINTAINABILITY

Service maintainability is defined as the mean time to restore service ($MTTR_s$) following a system service interruption.

$$MTTR_s = \frac{\text{Sum Total Time to Restore Service}}{\text{Number of Failures}}$$

$$MTTR_s = \left(1/NF_s\right)\sum_{i=1}^{NF_s} TTR_i$$

where:

TTR_i = Time to restore service following the *i*th service interruption (Downtime Interval)

NF_s = Number of failures, malfunctions, and operating disruptions classified as service interruptions during the Period of Operating Hours, OH_s

In computing the cumulative time to restore and the associated number of failures (NF_s), only service interruptions with Downtime Intervals greater than Grace Time (see Section 4.1) shall be included. However, once the specified maximum number of Grace Time allowances has been reached, no further Grace Time shall be allowed and all subsequent service interruptions shall be included in the calculation of Downtime Intervals. In addition, the Downtime Interval for each such event shall be the full time interval of cessation of service according to the following points:

1. The Grace Time shall not be subtracted from the TTR_i for a countable system service interruption.
2. The Downtime Interval shall be measured from the time of detection of the service interruption until the time of restoration of service for the specific train or

equipment that malfunctioned, whether the restoration is accomplished by automatic means, or by repair/replacement of the malfunctioning equipment.

4.3 SERVICE AVAILABILITY

Service Availability (A_s) is defined as follows:

$$A_s = \frac{MTBF_s}{MTBF_s + MTTR_s}$$

Service availability shall be calculated over a specified time interval. This calculation of service availability is equivalent to the actual operating hours (scheduled operating hours minus the accumulated downtime) divided by the scheduled operating hours.

5.0 AUTOMATIC TRAIN CONTROL

The automatic train control (ATC) subsystem shall provide automatic train protection (ATP), automatic train operation (ATO), and automatic train supervision (ATS) functions. ATP shall provide the primary protection for passengers, personnel, and equipment against the hazards of operations conducted under automatic control. ATP functions shall have precedence over both the ATO and ATS functions. ATO shall control basic operations that would otherwise be performed by an operator and does so within the protection limits imposed by ATP. The ATS shall provide system status information and the means for the Central Control operator to monitor and override the automatic control for various functions of the system.

For automatic people mover (APM) systems that utilize communications-based train control for ATC, the requirements of IEEE P1474.1–2004, *IEEE standard for communications-based train control (CBTC) performance and functional requirements,* shall apply in lieu of the requirements provided in Section 5.1 and Section 5.2.

5.1 AUTOMATIC TRAIN PROTECTION FUNCTIONS

All ATP functions shall be designed and implemented in accordance with Section 3.2, *Safety Principles,* and Section 3.3, *Automatic Train Control System Fail-Safe Design.*

5.1.1 Presence Detection

Presence detection shall be an ATP function if required to assure the protection aspects of other ATP functions, such as train separation assurance and/or guideway switch interlocks.

As an ATP function, presence detection shall be continuous in accordance with Section 5.1.7 in any and all automated areas of the guideway. All trains and any other vehicles that operate on the system in the presence of trains running in automatic operation shall be detected regardless of whether they are being operated in automatic or manual control.

The presence-detection function shall be reinitialized and all trains located and identified by positive detection prior to the resumption of automatic operation. In no case shall automatic operation be allowed based upon manual input of position data.

5.1.2 Separation Assurance

Separation assurance shall be a required ATP function for any APM system configuration that operates trains in following moves around the guideway.

Separation assurance shall provide protection against rear-end collisions for following trains by maintaining a zone at the rear of each train that continuously provides sufficient stopping distance for the following train assuming that the train ahead can stop instantaneously.

Stopping distance shall be calculated analytically using the cumulative "worst-case" characteristics of relevant elements, where worst case pertains to the characteristic of the element that results in maximum stopping distance. This includes, but is not limited to:

1. Maximum runaway acceleration
2. Minimum emergency braking condition
3. Maximum cumulative time delays
4. Maximum attainable overspeed
5. Grade
6. Worst-case load
7. Minimum adhesion/traction
8. Maximum design tailwind

For stopping distance calculation purposes, minimum emergency braking condition shall be based upon the single worst-case failure conditions of the braking system elements as determined by an appropriate analysis conducted in accordance with the requirements of Section 3.1.2.1, *Hazard Analyses.*

For APM systems that permit the automated operation of trains in opposing directions on the same track, separation assurance using calculated stopping distances for both trains shall apply for the prevention of head-on collisions.

For APM systems that employ automatic coupling, the coupling maneuver shall be permitted, provided the entire maneuver is conducted under the protection of ATP and can be verified and validated to be in accordance with Section 3.3, *Automatic Train Contol System Fail-Safe Design.*

For APM systems where the separation between successive trains is physically maintained, as it is in a

cable-propelled system, and where it can be shown by analysis according to Section 3.1.2.1, *Hazard Analyses,* that slippage and/or detachment from the physical mechanism is possible, then such slippage or detachment shall be detected and emergency braking shall be initiated to stop the slipping/detached train and all other trains connected to that mechanism.

Comparable separation assurance protection shall be required for APM systems that employ other means to maintain separation between successive trains.

5.1.3 Unintentional Motion Detection

Detection of unintentional motion shall be a required ATP function for all APM systems.

The ATP shall initiate emergency braking in the event a train is detected to be moving when it has not been commanded to move. Emergency braking shall also be initiated whenever a train is detected to be moving against the permitted travel direction (rollback).

5.1.4 Overspeed Protection

Overspeed protection shall be a required ATP function for all APM systems.

Guideway alignment, civil constraints, and train traffic conditions as determined by ATP shall define the speed limits that represent the maximum allowable train speed at any point on the guideway.

The overspeed protection function shall provide speed enforcement, ensuring that the speed of a train never exceeds the defined speed limit anywhere along the entire route. The overspeed protection equipment shall include speed-measuring devices that furnish signals that are a measure of the actual speed of the train. If ever the actual speed of the train exceeds the speed limit, the overspeed protection equipment shall immediately command emergency braking.

5.1.5 Overtravel Protection

Overtravel protection shall be a required ATP function for any APM system configuration that permits the automatic operation of trains up to or in close proximity to an end-of-guideway terminus.

Overtravel protection shall be incorporated into, or function in conjunction with, overspeed protection to prevent trains from overtraveling the end-of-guideway or, if buffers are specified, to prevent trains from exceeding the design limits for impact with an end-of-guideway buffer. Overtravel protection design shall be based on stopping distance calculations using cumulative "worst-case" characteristics of relevant elements as in Section 5.1.2 above.

5.1.6 Parted Consist Protection

Parted consist protection shall be an ATP function for APM systems that utilize separate vehicles coupled together in a consist of two or more vehicles to form a train. Parted consist protection shall be required regardless of whether the individual vehicles are considered to be permanently coupled or whether they are routinely uncoupled for maintenance or operational purposes.

Parted consist protection shall detect the uncoupling, detachment, and/or separation of vehicles in a consist, and shall thereupon immediately cause all vehicles of the previously connected train to brake to a full stop.

Presence detection, if applicable under the requirements of Section 5.1.1, shall detect the individual presence and precise location of each of the separated entities to the extent possible within the limits of the presence detection segmentation.

5.1.7 Lost Signal Protection

For all APM systems, all signals that are critical to the functions of ATP shall be continuous or be of such a repetitive nature that signal interruption is detected. Detection of signal interruption shall result in emergency braking by ATP in sufficient time so as not to compromise any safety aspect of the ATP functional design.

5.1.8 Zero Speed Detection

On APM systems where the trains are required to stop, zero speed detection shall be a required ATP function.

Zero speed shall not be registered until a speed of 0.30 meters per second (0.95 feet per second) or less is attained and braking is commanded.

5.1.9 Unscheduled Door Opening Protection

Unscheduled door opening protection shall be a required ATP function for all APM systems.

If any automatic door or emergency exit door on a train unlocks for any reason while the train is in motion (above zero speed as defined in Section 5.1.8), that train shall be caused to brake to a full stop.

For systems that include train/platform separation walls and automatic station doors, unscheduled door opening protection by ATP shall also apply. If any automatic station door is unlocked for any reason, trains shall be prohibited from entering or leaving that station platform. If any of these doors are unlocked for any reason as a train is entering or leaving the station platform area, the process of braking the train to a full stop shall be immediately initiated.

In the event of any unscheduled door opening (train or station), a local manual reset by authorized personnel shall be required prior to the restoration of automated train operation.

5.1.10 Door Control Protection Interlocks

Door control protection interlocks shall be provided by ATP on all APM systems.

These interlocks shall ensure that the following conditions are satisfied prior to enabling the automatic unlocking and opening of the train doors and, if provided, the station platform doors:

1. The train is "properly aligned" at a station platform per the criteria in Section 5.2.2.
2. Zero speed is detected.
3. Propulsion power is removed from the motors.
4. The train is positively constrained against motion.

For APM systems where trains do not achieve a complete stop for boarding and discharging passengers, the following conditions shall be satisfied for automatic unlocking and opening of train doors and station platform doors (if provided):

1. Speed shall not exceed 0.35 meters per second (1.1 feet per second).
2. Acceleration and jerk rates shall be limited to values determined to be acceptable by analysis according to the requirements of Section 3.1.2.1, *Hazard Analyses.*
3. The entire door opening and door closing sequence shall occur within the designated zones as determined by an analysis conducted in accordance with Section 3.1.2.1, *Hazard Analyses.*

5.1.11 Departure Interlocks

Departure interlocks shall be provided by ATP on all APM systems.

Any train stopped in a station shall not be permitted to move until all doors (train and station platform, if provided) are properly closed and locked. Only then shall the constraint against motion be removed and the power be applied to the propulsion motors.

For APM systems where trains do not achieve a complete stop for boarding and discharging passengers, departure interlocks shall be provided to stop the train from departing the station if all doors are not closed and locked.

5.1.12 Direction Reversal Interlocks

Travel direction reversal interlocks shall be provided by ATP on all APM systems requiring bidirectional operation on any segment of the automated guideway.

Any reversal of train travel direction shall occur only after zero speed has been registered (see Section 5.1.8). Reversing of train direction shall occur automatically at stations or terminal zones as required by the system configuration for the support of pinched loop, intermediate turnback loop, reverse direction loop, or shuttle modes of operation.

Any reversal of a train shall also be possible by remote manual command from the Central Control.

5.1.13 Propulsion and Braking Interlocks

Propulsion and braking interlocks shall be provided by ATP on all APM systems.

Emergency braking shall be "irrevocable," that is, once it is initiated, it shall remain activated until the train comes to a complete stop. After the train has stopped, the emergency braking shall be required to be reset for normal operation to resume. For situations where the method of reset is not specified by Section 5.0, *Automatic Train Control,* the method shall be determined by an analysis conducted in accordance with Section 3.1.2.1, *Hazard Analyses.* If conditions as determined by ATP are not correct for the train to move, the emergency braking shall remain applied regardless of any reset signals or actions, except that it shall be possible to switch to full manual operation, thus disabling the ATP functions of that train. If correct ATP conditions exist after irrevocability has been removed, the train shall be permitted to move, but if a subsequent malfunction occurs, the irrevocable emergency braking shall be applied as before.

The emergency braking controls shall be interlocked with the propulsion controls such that braking commands dominate.

5.1.14 Guideway Switch Interlocks

Guideway switch interlocks shall be provided by ATP for any APM system that operates trains under automatic control over a switch/switches installed along the guideway. For switching mechanisms on board the train, comparable interlocks that meet the intent of this section, as determined by analysis in accordance with the requirements of Section 3.1.2.1, *Hazard Analyses,* shall be provided.

ATP shall prevent a train from entering a switch that is not properly aligned and locked, and shall prevent a switch from becoming unlocked and/or moved once a train is committed to traversing it.

Control circuits shall be arranged so that an aligned and locked switch cannot be signaled for a route until each portion of the switch is verified to be in the correct position. When switch conditions are not correct (whether the switch has been activated automatically or manually), the control signals normally transmitted to approaching trains shall assure that any approaching train in automatic mode shall stop before reaching the entrance point of the switch.

Whenever a train is in the protected zone associated with a switch or a series of switches, route locking shall prevent the automatic or remote manual movement of any of the switches in the protected zone and shall prevent any conflicting train movements from occurring.

Presence detection locking shall be employed to prevent a switch from being moved if there is a train occupying it regardless of whether the switch is being operated under automatic or remote manual control.

Time locking (with approach release of that time locking optional) shall be employed in the switching circuits so that, if the section of guideway approaching a switch has been cleared for movement over that switch, the switch cannot be moved until a definite time has elapsed after the speed limit for the approaching section has been placed in a zero speed condition and the switch is not occupied. The time allowance shall be at least 10% greater than the time required for the train to traverse the stopping distance as calculated in accordance with Section 5.1.2. If the option of approach release of the time locking is used, then the time can be zero if there is no part of a train occupying the approach section. The length of the approach section for the switch shall be greater than the worst-case stopping distance computed for that specific guideway section.

ATP shall prevent the automatic or remote manual unlocking of a switch after a train has committed to traversing it until the train has cleared the switch. Protection against inadvertent release of locking due to momentary loss of power or train detection shall be provided.

5.2 AUTOMATIC TRAIN OPERATION FUNCTIONS

The ATO shall function to automatically operate trains about the system in accordance with prescribed operating criteria but within the safety constraints imposed by ATP.

5.2.1 Motion Control

The starting, stopping, and regulation of the train speed as it travels along the guideway shall be controlled by ATO so that the acceleration, deceleration, and jerk rates are within acceptable passenger comfort limits and the speed is maintained below the overspeed limits imposed by ATP.

5.2.2 Programmed Station Stop

Programmed station stops shall be made within acceptable passenger comfort limits. When boarding and discharging passengers, the train shall provide at all doors at least an 82 cm (32.5 inches) clear opening within the designated boarding zone. This opening shall allow egress only onto the platform.

If the train and station doors are misaligned by more than the distance permitted in the preceding paragraph, the doors shall not open automatically. An alarm shall be sent to Central Control.

5.2.3 Door and Dwell-Time Control

Train doors shall be automatically controlled by ATO during passenger boarding and discharging. If automatic station doors are provided, they shall be controlled as a set with matching train doors. Train and matching station doors, if provided, shall open and close together.

It shall be possible to manually disable the operation of any door set (on the train or at the station) without affecting the automatic operation of other unaffected sets. When automatic station doors are provided and a door set (train/station) is disabled, then the matching set shall also be disabled with respect to automatic operations but without the need for manual intervention.

If any doors fail to open or fail to close within 10 seconds of being commanded to do so, an alarm shall be sent to Central Control.

The amount of time the train remains in the station with doors open shall be established by the designer and automatically controlled by ATS as a function of fully automated operation. Once door open time has expired and any “hold door open” commands initiated by ATS or the Central Control operator have been removed, all doors shall be commanded to close.

When a train under manual control is properly berthed in a station and the train operator commands the train doors to open or close, the corresponding station doors, if provided, shall also open or close.

5.3 AUTOMATIC TRAIN SUPERVISION FUNCTIONS

Automatic Train Supervision shall monitor and manage the overall operation of the system. ATS shall provide the interface between the system and the Central Control operator. Through audio and visual displays, information shall be presented describing the status of the system on a real-time basis. This information shall allow the Central Control operator to assess conditions throughout the system and to take appropriate actions. The Central Control operator shall be able to issue commands to initiate and terminate system operations, override selected automatic commands and operations, and perform other system management functions.

For APM systems where there is no operator physically located in Central Control, alarms and malfunction information must be transmitted to a responsible individual authorized to respond to the situation in a timely manner.

5.3.1 Constraints on Automatic Train Supervision

Should ATS become completely inoperative for any reason, ATP and ATO shall remain operable unless a

system shutdown is commanded by the Central Control operator. Emergency controls on the Central Control console shall, independent of the ATS equipment, provide at least the following system emergency shutdown functions:

1. All trains stop
2. All propulsion power shut off

5.3.2 Status and Performance Monitoring

System status and performance information shall be presented to the Central Control operator by way of functionally separate displays, the *System Operations Display* and the *Power Schematic Display.*

5.3.2.1 System Operations Display

The System Operations Display (SOD) shall provide a visual representation of real-time operating conditions throughout the system. The display design shall:

1. Be of sufficient size and/or quantity and display resolution to be viewed with ease from the normal seating area at the Central Control operator consoles.
2. Show approximate geographical representations of the guideway and the locations of relevant physical features such as passenger stations, switches, and/or maintenance and storage facilities.
3. Dynamically depict any of the following system operating conditions that are pertinent to the system configuration:
   a. The location and identification of all trains in all parts of the system designed for automatic operation
   b. The direction of travel of all active trains
   c. The number of cars comprising each train (if train consist is variable)
   d. The train identification number used to interact with the train (if train identification is not obvious from the system configuration)
   e. The status of any switches in the system
   f. The operating mode and status of selected system equipment
   g. The status of each station including the current active dwell for each station
4. Incorporate such other visual aids as may be necessary to permit the Central Control operator(s) to manage the system efficiently.

5.3.2.2 Power Schematic Display

The Power Schematic Display (PSD) shall provide a visual indication of the power distribution system status throughout the system. The PSD shall be of sufficient size and/or quantity and display resolution to be viewed with ease from the normal seating area at the Central Control operator console(s).

The PSD shall clearly display the following conditions as a minimum:

1. The presence or absence of electrical power in each propulsion power circuit, which may be individually energized or de-energized.
2. The presence or absence of any power distributed along the guideway by guideway segment for each power segment that may be individually energized or de-energized.
3. The status of all circuit breakers and/or switches in the power supply system. Any tripped condition shall be alarmed.
4. The presence or absence of backup power.
5. The presence of any alarm condition.

Indication of power status shall be by both voltage monitoring and device position indication. PSD indication and control functions shall not be affected by any single point failure.

5.3.3 Performance Control and Override

Management and operation of the system shall be accomplished by the control and override functions. There shall be both automatically controlled and manually initiated control and override functions as described in this section.

5.3.3.1 Automatic Control Functions

To the extent warranted, the ATS system shall perform the control and coordination functions necessary to achieve fully supervised automatic operation of the system.

5.3.3.1.1 Mode Management: The ATS shall manage all specified modes of operation. Available modes shall depend upon system technology, guideway configuration, operating plan, and failure mode recovery plan.

5.3.3.1.2 Train Tracking: The ATS shall systematically track each train around the system to the extent warranted by the system configuration and in a manner that is consistent with the requirements for management of the specified modes of operation.

5.3.3.1.3 Headway Management: Consistent with the selected mode of operation and the specified degree of interactive train regulation, the ATS shall act to maintain the required time (as measured at a fixed point on the guideway) and/or distance spacing between trains in automatic operation on the system.

5.3.3.1.4 Train Routing: The ATS shall automatically accomplish all routing functions required by the

selected mode of operation. This shall include initiating route, switch position, and travel direction reversal requests, as required.

5.3.3.2 Manual Control and Override Functions

The capabilities and functions described in this section shall be incorporated in the Central Control console. Controls and displays associated with ATC shall be integrated with the controls and displays of the communications (see Section 6.0, *Communications*) and electrical (see Section 5.3.2.2, *Power Schematic Display*) subsystems so as to facilitate the efficient/effective supervision of all subsystems by one operator at the console.

Manual controls shall be provided that enable the Central Control operator to perform the following functions:

1. *Train Dispatching:* The Central Control operator shall be able to dispatch trains into service from any designated off-line launch point.
2. *Train Routing:* Depending upon the system configuration, the ATS shall be designed so that each train can be assigned to a specific operating mode, lane, or route, via an instruction from the Central Control operator.
3. *Initiation of Service:* The Central Control operator shall be able to initiate system service.
4. *Termination of Service:* The Central Control operator shall be able to terminate system service.
5. *Modify Train Operations:* The Central Control operator shall be able to issue commands that modify normal train operation.
6. *Remove Trains:* For systems that provide off-line storage, the Central Control operator shall be able to direct a train to proceed out of service.
7. *Initiate Failure Mode Operations:* The Central Control operator shall be able to convert the system from its normal operating mode to any available alternative operating mode for failure management purposes.
8. *Hold Trains:* The Central Control operator shall be able to command trains to hold in the stations.
9. *Command Switches:* When switches are provided, the Central Control operator shall be able to individually command switches to move.
10. *Stop All Trains:* The Central Control operator with one command shall be able to stop all trains on the guideway.
11. *Command Power Off/On:* The Central Control operator shall be able to command propulsion power off/on to the entire system or to individual power circuits, depending upon the segmentation provided.
12. *Acknowledge and Process Alarms:* The Central Control operator shall be able to receive from several subsystems, acknowledge, store, and recall alarm message displays and acknowledge accompanying audible alarms.

Except for a single-event command, once a command is imposed by the Central Control operator and accepted by ATS, the action shall remain operative until subsequently removed by the operator.

5.3.3.3 Alarms and Malfunction Reporting

Major system components shall be automatically monitored and alarms shall be annunciated for malfunctions and failures thereof. Also, system-related facilities shall be monitored and alarms annunciated for fire/life safety problems and/or security intrusions. The Central Control console shall incorporate both an incident (message) display and audible alarms for the benefit of the Central Control operator. Within two seconds of detection, the occurrence of an incident or condition shall be reported on a display, indicating the time of the incident, the nature and classification of the incident or condition, the identification of the vehicle and train, and/or the specific guideway or station location involved. Each alarm shall be indexed and time-tagged as to when the fault was detected. Alarms shall be stored and have the capability of being recalled/redisplayed by an index number or by the hardware type with which it is associated (e.g., train, substation, passenger station, switch). Acknowledgement of the alarm by the Central Control operator shall cause the audible alarm to cease; however, the associated alarm indication shall persist until the condition is cleared. All alarm reports and clearing shall be recorded in memory and printed on a line printer.

Data communications between Central Control and trains shall be maintained and confirmed. Failure of any train to respond shall be alarmed and annunciated at Central Control.

5.3.3.3.1 System Alarms: System operation malfunctions, alarms, and reporting shall be primarily for security, safety, and unscheduled stoppage problems.

As a minimum, system operations malfunctions shall be reported in one of two priority classifications, as described below. The level of classification and reporting of faults shall be sufficiently detailed to allow operating and maintenance personnel to make rational decisions in reacting to the reports, consistent with the functions required of them in the operation and maintenance plans, procedures, and manuals.

Priority I malfunctions are those that pose an immediate threat to passenger safety and/or the threat of damage to system equipment.

Priority II malfunctions are those that do not pose an immediate threat but could cause a potential threat to passengers or equipment if not corrected quickly.

5.3.3.3.2 Facility Fire and Intrusion Alarms: Facility fire/smoke and intrusion alarms, if provided, shall be annunciated separately and redundantly (audibly and visually) on the Central Control console. The location of the alarm point shall be indicated.

5.3.3.4 Data Recording and Reporting

The ATS subsystem shall include the recording of selected data transactions between Central Control and other portions of the system. Such data shall be recorded in a format that includes the date and exact time of each data transmission. Data shall be recorded and stored on appropriate media in a format suitable for both a permanent file and random access retrieval and for use with system data processing software to produce reports, if provided.

If specified, an appropriate subset of this recorded data shall be able to be printed in real time on a printer at Central Control. This printout shall constitute the Daily Operations Log.

5.4 MANUAL OPERATION LIMITATIONS

These APM Standards are intended for fully automatic operation and do not apply to extended passenger service in manual mode. Manual mode operation may be used for testing, recovery, maintenance, and system failures/failure management, or other abnormal conditions. The *Hazard Resolution Process* of Section 3.1.2 shall address the hazards introduced by manual operation.

For limited manual operation, the design shall enable the operator(s) to observe guideway conditions, communicate with Central Control and passengers, observe vehicle status indications, and control vehicle propulsion, braking, and doors. When not in use, the controls and status indicators shall be protected from access by passengers.

6.0 AUDIO AND VISUAL COMMUNICATIONS

All audio and visual communications equipment shall operate independently of guideway power and shall function fully under the ambient conditions to which it may be exposed. All audio and visual communications equipment required by this standard shall be powered by uninterruptible power for a time period as determined by an analysis in accordance with Section 3.1.2.1, *Hazard Analyses.*

6.1 AUDIO COMMUNICATION

Facilities and equipment shall be provided to permit voice communications between the Central Control Operator and (1) passengers, and (2) operations and maintenance personnel located throughout the System.

All audio communication systems and public address systems required herein shall meet the requirements of Section 6.1.6.

6.1.1 Station Public Address

A station public address system shall enable live announcements to be made from Central Control to all public areas of all station platforms.

Live messages shall override any prerecorded messages, if provided. All speakers in a given station zone shall deliver announcements simultaneously when that station or zone is selected. The public address system zoning shall provide full coverage to all public areas of each station.

6.1.2 Emergency Station and Wayside Communications

There shall be two-way emergency audio communications linking Central Control with all passenger stations and any Blue Light Stations (as specified by Section 11.4.1, *Standard for Fixed Guideway Transit and Passenger Rail Systems,* NFPA 130–2003). Each Emergency Communication Device (ECD) shall automatically call Central Control when activated. A display at Central Control shall identify the communicating ECD and indicate whether there are any additional activated ECDs.

All ECD equipment shall be of heavy duty, vandal-resistant design, including a tamper- and weather-resistant enclosure. These emergency audio communications shall be independent of any other communication system. The person operating the ECD shall receive an audible indication that the unit is calling. Instructions for use shall be provided in vandal-resistant signs integral with or adjacent to the ECDs.

6.1.3 Train Voice Communications and Public Address

A full-duplex communications system shall be provided to permit two-way voice communications between the Central Control Operator and passengers or personnel within each passenger compartment of each train. Full coverage of all trains throughout the System shall be provided. Activation of two-way voice communications between Central Control and the trains shall be possible only from Central Control. Passenger-initiated communications requests from a train, including the passenger compartment identification

number, shall automatically be displayed at Central Control for the Central Control Operator to activate the communications link. The display shall also show any queue of such communication requests. The Central Control Operator shall be able to activate this link upon receiving an indication of a passenger-initiated communications request or at any other time to receive communications. A passenger-initiated communications request shall include an audio and visual onboard indication that the call has been requested.

A train public address function shall be provided for the Central Control Operator in two modes: (1) to make audible announcements in all passenger compartments of any one train, and (2) to make audible announcements in all passenger compartments of all trains in the System. Live messages shall override any prerecorded messages, if provided. Speaker fire resistance shall meet the requirements of *Commercial Audio Equipment,* UL 813–1993. Full coverage of all trains throughout the System shall be provided. For trains that can be operated in manual mode, a means shall be provided to enable the train operator to make announcements throughout the train.

6.1.4 Operations and Maintenance Personnel Communications

The APM System shall include an internal telephone/intercom system connecting Central Control, all administrative offices and maintenance areas, and selected storage and equipment rooms. Telephones/intercoms not otherwise protected shall be of heavy-duty, vandal-resistant design, including a tamper- and weather-resistant enclosure.

An O&M radio system shall be provided for communications between the Central Control Operator and O&M personnel. Each O&M person on duty not having direct access to the internal telephone/intercom system shall have a portable radio at all times.

6.1.5 Recording of Audio Transmissions

An audio recording device shall be provided to record all communications over train voice communications, ECDs, and public address systems with the Central Control Operator. This device shall be capable of individually recording at least 24 hours of continuous audio for each audio communication system described in Section 6.1.1 through Section 6.1.3 with indication of date and time. Recording media shall be provided so that each day's recording can be stored.

6.1.6 Intelligibility of Audio Communications

The required audio communications systems shall meet the following:

1. Station public address systems, emergency station and wayside communications systems, and the internal O&M telephone/intercom system shall meet the intelligibility requirements of NFPA 72–2002. In meeting the intelligibility requirements, measurement conditions shall represent the entire passenger space of the station or the position of the telephone/intercom and provide the average result of all reflected signals and reverberations, and all auxiliary systems shall be in normal operation, such that the ambient noise will be at typical maximum levels. The tests of telephones/intercoms shall be repeated for a representative number of locations throughout the System.
2. All wireless voice communications between the wayside and the trains, including Central Control, shall meet DAQ 3 of Table 1, Annex-A of TIA/EIA Telecommunications Systems Bulletin, *Wireless communications systems–performance in noise and interference–limited situations–recommended methods for technology–independent modeling, simulation, and verification,* TSB-88, January 2002, for 97% of the trainway. In areas of the trainway where DAQ 3 is met, the intelligibility shall meet the intelligibility requirements of NFPA 72-2002. The vehicle interior noise shall be at least at the maximum interior level as measured in accordance with Part 2, Section 7.7.4. This test shall be repeated for a representative number of locations throughout the System.
3. All voice communications exclusively within a train shall meet the intelligibility requirements of NFPA 72–2002. The vehicle interior noise shall be at least at the maximum interior level as measured in accordance with Part 2, Section 7.7.4.
4. The O&M radio system shall provide signal coverage greater than or equal to DAQ 3, as referenced in (2) above, for 97% area coverage reliability within the System where O&M personnel may work.

6.2 VIDEO SURVEILLANCE

A closed-circuit television (CCTV) subsystem shall be provided and installed to permit Central Control to monitor passenger activities on all station platforms in the System, particularly the boarding areas and along the entire edge of any open platforms. Video surveillance is not required for attended station platforms.

6.2.1 Central Control Equipment

Central Control shall be equipped with monitors for displaying camera outputs, organized in a logical order with identifications displayed on each screen to orient the Central Control Operator and facilitate identification of the image location.

Closed-circuit televison monitors shall provide a clear picture in the ambient light level of the Central Control room.

6.2.2 Passenger Station Equipment

Cameras shall have a "usable picture" with scene illumination from 0.3 Lux (0.03 foot-candles) up to bright sunlight, using automatic light compensation. Cameras shall be tamper-proof and vandal-resistant. Cameras shall automatically adjust to the environmental and the ambient light conditions of each station throughout the operating day.

Camera position for platform viewing, particularly the boarding areas and along the entire edge of any open platforms, shall be fixed and shall not be remotely controlled. Camera mounts and any housings shall be tamper-proof and vandal-resistant for all applications and weather-resistant for outdoor applications.

6.2.3 Recording of Video Transmissions

A system shall be provided to record the image of each camera in the system, but not necessarily all cameras simultaneously, to include identification of the camera, time, and date.

6.3 PASSENGER INFORMATION DEVICES

The following audio announcements and dynamic signs are required for APM systems.

6.3.1 Vehicle

Each passenger compartment shall have automatic on-board audible announcements that signal each station as it is approached to inform passengers of the impending stop. For APM systems having trains operating over more than one route from the same platform, audio announcements shall indicate the name of the station.

For APM systems having trains operating over more than one route from the same platform, dynamic signs shall be provided for each passenger compartment that indicate train route and/or destination and the name of the station at which the train is approaching or has stopped. These dynamic signs shall be positioned for maximum visibility by passengers.

6.3.2 Stations

Each station platform shall be provided with automatic audible and visual warnings that signal the arrival and departure of trains. The arrival warning shall be made before the train enters the station. The departure warning indicating that the doors are about to be closed shall be communicated to passengers both in the trains and on the platform. APM systems where trains do not achieve a complete stop for boarding and discharging passengers shall provide warnings that meet an equivalent facilitation in accordance with Section 3.1.2.1, *Hazard Analyses.* APM systems having trains operating over more than one route from the same platform shall also audibly announce train route and/or destination.

For APM systems having trains operating over more than one route from the same platform, dynamic station signs shall be provided on each station platform to inform passengers of train route and/or destination. The vehicle dynamic sign may satisfy this requirement provided that the message is also posted on the exterior of the vehicle and can be read by passengers on the station platform.

ANNEX A

System Safety Program Requirements

THIS ANNEX IS A MANDATORY PART OF THE STANDARD

(As indicated in Section 3.0, *Safety Requirements,* equivalent techniques may be used in place of the techniques outlined in this annex.)

A.1 SYSTEM SAFETY PROGRAM PLAN

A.1.1 Purpose

The System Safety Program Plan (SSPP) shall describe in detail tasks and activities of system safety management and system safety engineering required to identify, evaluate, and eliminate/control hazards, or reduce the associated risk to a level acceptable to the authority having jurisdiction throughout the system life cycle.

A.1.2 Description

The SSPP shall be developed to provide a basis of understanding as to how the system safety program will be accomplished to meet safety requirements. The approved plan shall, on an item-by-item basis, account for all required tasks and responsibilities. The SSPP shall include the following:

A.1.2.1 Program Scope and Objectives

Each SSPP shall describe, as a minimum, the four elements of an effective system safety program: a planned approach for task accomplishment, qualified people to accomplish tasks, authority to implement tasks through all levels of management, and appropriate commitment of resources (both staffing and funding) to assure tasks are completed. The SSPP shall define a program to satisfy the system safety requirements. This section shall:

1. Describe the scope of the overall program and the related system safety program.
2. List the tasks and activities of system safety management and engineering. Describe the interrelationships between system safety and other functional elements of the program. List the other program requirements and tasks applicable to system safety. Identify where they are specified or described.
3. Account for all required safety tasks and responsibilities. A matrix shall be provided to correlate the requirements to the location in the SSPP where the requirement is addressed.

A.1.2.2 System Safety Organization

The SSPP shall describe:

1. The system safety organization or function within the organization of the total program, using charts to show the organizational and functional relationships, and lines of communication. The organizational relationship between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization shall be shown. Review and approval authority of applicable tasks by system safety shall be described.
2. The responsibility and authority of system safety personnel, other organizational elements involved in the system safety effort, and system safety groups. Describe the methods by which safety personnel may raise issues of concern directly to the program manager or the program manager's supervisor within the corporation. Identify the organizational unit responsible for executing each task. Identify the authority in regard to resolution of all identified hazards.
3. The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources, and a summary of the qualifications of key system safety personnel assigned to the effort, including those who possess coordination/approval authority for prepared documentation.
4. The procedures for the integration and coordination of the system safety efforts, including assignment of the system safety requirements to action organizations, coordination of system safety programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.
5. The process through which management decisions will be made, including timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, program deviations, and so on.
6. Details of how resolution and action relative to system safety will be effected at the program management level possessing resolution authority.

A.1.2.3 System Safety Program Milestones

The SSPP shall:

1. Define system safety program milestones. Relate these to major program milestones, program element responsibility, and required inputs and outputs.
2. Provide a program schedule of safety tasks including start and completion dates, reports, and reviews.
3. Identify subsystem, component, and software safety activities as well as integrated system-level activities (i.e., design analyses, tests, and demonstrations) applicable to the system safety program but specified in other engineering studies and development efforts to preclude duplication.

4. Provide the estimated manpower loading required to complete each task.

A.1.2.4 General System Safety Requirements and Criteria

The SSPP shall:

1. Describe general engineering requirements and design criteria for safety. Describe safety requirements for support equipment and operational safety requirements for all appropriate phases of the life cycle up to, and including, disposal. List the safety standards and system specifications containing safety requirements that shall be complied with. Include titles, dates, and where applicable, paragraph numbers.
2. Describe the risk assessment procedures. The hazard severity categories, hazard probability levels, and the system safety precedence that shall be followed to satisfy the safety requirements of the program. State any qualitative or quantitative measures of safety to be used for risk assessment, including a description of the acceptable/unacceptable risk levels. Include system safety definitions that modify, deviate from, or are in addition to those in this standard.
3. Describe closed-loop procedures for taking action to resolve identified unacceptable risk, including those involving nondevelopmental items.

A.1.2.5 Hazard Analysis

The SSPP shall describe:

1. The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met.
2. The depth within the system to which each technique is used, including hazard identification associated with the system, subsystem, components, software, hazardous materials, personnel, ground support equipment, nondevelopmental items, facilities, and their interrelationship in the logistic support, training, maintenance, operational, and disposal (including render safe and emergency disposal) environments.
3. The integration of hazard analyses performed by others with overall system hazard analyses.
4. Efforts to identify and control hazards associated with materials used during the system's life cycle.

A.1.2.6 System Safety Data

The SSPP shall:

1. Describe the approach for collecting and processing pertinent historical hazard, mishap, and safety lessons learned, and data.
2. Identify deliverable data by title and number, and means of delivery (e.g., hard copy, electronically).
3. Identify nondeliverable system safety data and describe the procedures for accessibility by the authority having jurisdiction and retention of data of historical value.

A.1.2.7 Safety Verification

The SSPP shall describe:

1. The verification (test, analysis, inspection, etc.) requirements for making sure that safety is adequately demonstrated. Identify any certification requirements for software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).
2. Procedures for making sure safety-related verification information is transmitted to the authority having jurisdiction for review and analysis.
3. Procedure for ensuring the safe conduct of all tests.

A.1.2.8 Audit Program

The SSPP shall describe the techniques and procedures to be employed to make sure the objectives and requirements of the system safety program are being accomplished.

A.1.2.9 Training

The SSPP shall describe the safety training for engineering, technician, operating, and maintenance personnel.

A.1.2.10 Incident Reporting

The SSPP shall describe the mishap/incident alerting/notification, investigation, and reporting process including notification of the authority having jurisdiction.

A.1.2.11 System Safety Interfaces

The SSPP shall identify, in detail:

1. The interface between system safety, systems engineering, and all other support disciplines such as: maintainability, quality control, reliability, software development, human factors engineering, medical support (health hazard assessments), and any others.
2. The interface between system safety and all system integration and test disciplines.

A.2 PRELIMINARY HAZARD ANALYSIS

A.2.1 Purpose

The Preliminary Hazard Analysis (PHA) shall identify safety critical areas, provide an initial assessment of hazards, and identify requisite hazard controls and follow-on actions.

A.2.2 Description

A preliminary hazard analysis shall be performed and documented to obtain an initial risk assessment of a concept or system. Based on the best available data, including mishap data (if assessable) from similar systems and other lessons learned, hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to the authority having jurisdiction shall be included. The PHA shall consider the following for identification and evaluation of hazards as a minimum:

1. Hazardous components (e.g., fuels, propellants, lasers, toxic substances, hazardous construction materials, pressure systems, and other energy sources).
2. Safety-related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This shall include consideration of the potential contribution by software (including software developed by other sources) to subsystem/system mishaps. Safety design criteria to control safety critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or other designated undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.
3. Environmental constraints including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects).
4. Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering; human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials; effects of noise or radiation on human performance). Those test unique hazards that will be a direct result of the test and evaluation of the article or vehicle.
5. Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, proof/testing of hazardous systems/assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials/wastes; radiation or noise emitters; electrical power sources) and training (e.g., training and certification pertaining to safety operations and maintenance).
6. Safety-related equipment, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail-safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).
7. Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.

A.3 SUBSYSTEM HAZARD ANALYSIS

A.3.1 Purpose

The Subsystem Hazard Analysis (SSHA) shall:

1. Verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents.
2. Identify previously unidentified hazards associated with the design of subsystems including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem.
3. Recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels.

A.3.2 Description

A subsystem hazard analysis shall be performed and documented to identify all components and equipment that could result in a hazard or whose design does not satisfy contractual safety requirements. Areas to consider are performance, performance degradation, functional failures, timing errors, design errors or defects, or inadvertent functioning. The human shall be considered a component within a subsystem, receiving both inputs and initiating outputs, during the conduct of this analysis.

The analysis shall include a determination:

1. Of the modes of failure, including reasonable human errors as well as single-point and common-mode failures, and the effects on safety when failures occur in subsystem components.
2. Of potential contribution of hardware and software (including that which is developed by other sources) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.
3. That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.

4. That the method of implementation of hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has it introduced any new hazards or risks.
5. Of the implementation of safety design requirements from top level specifications to detailed design specifications for the subsystem. The implementation of safety design requirements developed as part of the PHA shall be analyzed to ensure that it satisfies the intent of the requirements.
6. Of test plan and procedure recommendations to integrated safety testing into the hardware and software test programs.
7. That system-level hazards attributed to the subsystem are analyzed and that adequate control of the potential hazard is implemented in the design.

When software to be used in conjunction with the subsystem is being developed, the individual(s) performing the SSHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SSHA.

The SSHA shall be updated as a result of any system design changes, including software design changes, that affect system safety.

A.4 SYSTEM HAZARD ANALYSIS

A.4.1 Purpose

The System Hazard Analysis (SHA) shall:

1. Verify system compliance with safety requirements contained in system specifications and other applicable documents.
2. Identify previously unidentified hazards associated with the subsystem interfaces and system functional faults.
3. Assess the risk associated with the total system design, including software, and specifically of the subsystem interfaces.
4. Recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

A.4.2 Description

A system hazard analysis shall be performed and documented to identify hazards and assess the risk of the total system design, including software, and specifically of the subsystem interfaces.

This analysis shall include a review of subsystem interrelationships for:

1. Compliance with specified safety design criteria.
2. Possible independent, dependent, and simultaneous hazardous events including systems failures, failures of safety devices, common cause failures and events, and system interactions that could create a hazard or result in an increase in mishap risk.
3. Degradation in the safety of a subsystem or the total system from normal operation of another subsystem.
4. Design changes that affect subsystems.
5. Effects of reasonable human errors.
6. Determination:
   a. Of potential contribution of hardware and software (including that which is developed by other sources, or Commercial Off-The-Shelf hardware or software) events, faults, and occurrences (such as improper timing) on safety of the system.
   b. That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.
   c. That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of the system nor has it introduced any new hazards.

The SHA may be combined with and/or performed using similar techniques to those used for the SSHA.

When software to be used in conjunction with the system is being developed, the individual(s) performing the SHA shall monitor, obtain, and use the output of each phase of the formal software development process in evaluating the software contribution to the SHA.

The SHA shall be updated as a result of any system design changes, including software design changes, that affect system safety.

A.5 OPERATING AND SUPPORT HAZARD ANALYSIS

A.5.1 Purpose

The Operating and Support Hazard Analysis (O&SHA) shall evaluate activities for hazards or risks introduced into the system by operational and support procedures and evaluate adequacy of operational and support procedures used to eliminate, control, or abate identified hazards or risks.

A.5.2 Description

An O&SHA shall be performed to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering:

1. The planned system configuration/state at each phase of activity.
2. The facility interfaces.
3. The planned environments (or ranges thereof).
4. The supporting tools or other equipment, including software-controlled automatic test equipment,

specified for use; operational/task sequence; concurrent task effects; and limitations.
5. The potential for unplanned events including hazards introduced by human errors.

The human shall be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis. The O&SHA must identify the safety requirements (or alternatives) needed to eliminate or control identified hazards, or to reduce the associated risk to a level that is acceptable under either regulatory or contractually specified criteria.

The analysis shall identify:

1. Activities that occur under hazardous conditions, their time periods, and the actions required to minimize risk during these activities/time periods.
2. Changes needed in functional or design requirements for system hardware/software, facilities, tooling, or support/test equipment to eliminate or control hazards or reduce associated risks.
3. Requirements for safety devices and equipment, including personnel safety and life support equipment.
4. Warnings, cautions, and special emergency procedures (e.g., egress, rescue, escape), including those necessitated by failure of a computer software-controlled operation to produce the expected and required safe result or indication.
5. Requirements for packaging, handling, storage, transportation, maintenance, and disposal of hazardous materials.
6. Requirements for safety training and personnel certification.
7. Effects of nondevelopmental hardware and software across the interface with other system components or subsystems.
8. Potentially hazardous system states under operator control.

The O&SHA shall document system safety assessment of procedures involved in: system production, deployment, installation, assembly, test, operation, maintenance, servicing, transportation, storage, modification, demilitarization, and disposal.

The O&SHA shall be updated as a result of any system design or operational changes.

This page intentionally left blank

ANNEX B

Bibliography

THIS ANNEX IS INFORMATIVE AND NOT A MANDATORY PART OF THE STANDARD

Refer to the following for examples and guidance in the conduct of associated activities of the system safety programs:

1. American Public Transportation Association. (1999). *Manual for the development of rail transit system safety program plans.*
2. AREMA. *Signal manual.* Part 17.
3. EN 50126 / IEC 62278: *Railway applications—The specification and demonstration of reliability, availability, maintainability and safety (RAMS).* (September 1999). CENELEC, Central Secretariat: rue de Stassart 35, B—1050 Brussels.
4. EN 50128 / IEC 62279: *Railway applications—Communications, signaling and processing systems—Software for railway control and protection systems.* (March 2001). CENELEC, Central Secretariat: rue de Stassart 35, B—1050 Brussels.
5. EN 50129: *Railway applications—Communications, signaling and processing systems—Safety related electronic systems for signaling.* (February 2003). CENELEC, Central Secretariat: rue de Stassart 35, B—1050 Brussels.
6. U.S. Nuclear Regulatory Commission. (January 1981). *Fault tree handbook.* Report Number NUREG-0492.
7. *Handbook for transit safety and security certification,* DOT-FTA-MA-90–5006–02–01, DOT-VNTSC-FTA-02–12.
8. IEC 61508–1:1998: *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 1: General requirements.*
9. IEC CDIS 61508–2, Edition 1. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 2: Requirements for electrical/electro/programmable electronic safety-related systems.*
10. IEC 61508–3:1998. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 3: Software requirements.*
11. IEC 61508–4:1998. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 4: Definitions and abbreviations.*
12. IEC 61508–5:1998. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 5: Examples of methods for the determination of safety integrity levels.*
13. IEC 61508–6, Edition 1. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 6: Guidelines on the application of parts 2 and 3.*
14. IEC 61508–7:1998. *Functional safety of electrical/electro/programmable electronic safety-related systems. Part 7: Overview of techniques and measures.*
15. IEEE Std 1012–1986. *IEEE standard for software verification and validation plans.*
16. IEEE Std 1059–1993. *IEEE guide for software verification and validation plans.*
17. IEEE Std 1483–2000. *IEEE standard for verification of vital functions in processor-based systems used in rail transit control.*
18. *System safety analysis handbook.* (1997). 2nd Edition, System Safety Society, Sterling, Va.

This page intentionally left blank

INDEX