

Automated People Mover Standards

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

Documents

Document Sharing Hub



American Society of Civil Engineers

Automated People Mover Standards

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



Documents
Document Sharing Hub

Library of Congress Cataloging-in-Publication Data

Automated people mover standards / American Society of Civil Engineers.

pages cm

“ASCE Standard ANSI/ASCE/T&DI 21-13.”

Includes bibliographical references and index.

ISBN 978-0-7844-1298-5 (pbk.) – ISBN 978-0-7844-7787-8

(e-book)

1. Personal rapid transit – Standards. I. American Society of Civil Engineers.

TA1207.A95 2013

625.6–dc23

2013014955

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

This standard was developed by a consensus standards development process that has been accredited by the American National Standards Institute (ANSI). Accreditation by ANSI, a voluntary accreditation body representing public and private sector standards development organizations in the United States and abroad, signifies that the standards development process used by ASCE has met the ANSI requirements for openness, balance, consensus, and due process.

While ASCE’s process is designed to promote standards that reflect a fair and reasoned consensus among all interested participants, while preserving the public health, safety, and welfare that is paramount to its mission, it has not made an independent assessment of and does not warrant the accuracy, completeness, suitability, or utility of any information, apparatus, product, or process discussed herein. ASCE does not intend, nor should anyone interpret, ASCE’s standards to replace the sound judgment of a competent professional, having knowledge and experience in the appropriate field(s) of practice, nor to substitute for the standard of care required of such professionals in interpreting and applying the contents of this standard.

ASCE has no authority to enforce compliance with its standards and does not undertake to certify products for compliance or to render any professional services to any person or entity.

ASCE disclaims any and all liability for any personal injury, property damage, financial loss, or other damages of any nature whatsoever, including without limitation any direct, indirect, special, exemplary, or consequential damages resulting from any person’s use of, or reliance on, this standard. Any individual who relies on this standard assumes full responsibility for such use.

ASCE and American Society of Civil Engineers—Registered in U.S. Patent and Trademark Office.

Photocopies and permissions. Permission to photocopy or reproduce material from ASCE publications can be obtained by sending an e-mail to permissions@asce.org or by locating a title in ASCE’s online database (<http://cedb.asce.org>) and using the “Permission to Reuse” link.

Copyright © 2013 by the American Society of Civil Engineers.
All Rights Reserved.

ISBN 978-0-7844-1298-5 (paper)

ISBN 978-0-7844-7787-8 (PDF)

Manufactured in the United States of America.

20 19 18 17 16 15 14 13

1 2 3 4 5



Documents

Document Sharing Hub

STANDARDS

In 2006, 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
- ASCE/EWRI 2-06 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 and Specification for Masonry Structures: Containing Building Code Requirements for Masonry Structures (TMS 402-11/ACI 530-11/ASCE 5-11), Specification for Masonry Structures (TMS 402-11/ACI 530-11/ASCE 6-11), and Companion Commentaries
- ASCE/SEI 7-10 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 12-13 Guideline for the Design of Urban Subsurface Drainage
- ASCE/EWRI 13-13 Standard Guidelines for Installation of Urban Subsurface Drainage
- ASCE/EWRI 14-13 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)
- AF & PA/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 19-10 Structural Applications of Steel Cables for Buildings
- ASCE 20-96 Standard Guidelines for the Design and Installation of Pile Foundations
- ANSI/ASCE/T&DI 21-13 Automated People Mover Standards—Part 1
- 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
- ASCE/SEI/SFPE 29-05 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 33-09 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



STANDARDS

- 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
- ASCE/EWRI 39-03 Standard Practice for the Design and Operation of Hail Suppression Projects
- ASCE/EWRI 40-03 Regulated Riparian Model Water Code
- ASCE/SEI 41-06 Seismic Rehabilitation of Existing Buildings
- 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
- ASCE/SEI 48-11 Design of Steel Transmission Pole Structures
- ASCE/SEI 49-12 Wind Tunnel Testing for Buildings and Other Structures
- ASCE/EWRI 50-08 Standard Guideline for Fitting Saturated Hydraulic Conductivity Using Probability Density Functions
- ASCE/EWRI 51-08 Standard Guideline for Calculating the Effective Saturated Hydraulic Conductivity
- ASCE/SEI 52-10 Design of Fiberglass-Reinforced Plastic (FRP) Stacks
- ASCE/G-I 53-10 Compaction Grouting Consensus Guide
- ASCE/EWRI 54-10 Standard Guideline for Geostatistical Estimation and Block-Averaging of Homogeneous and Isotropic Saturated Hydraulic Conductivity
- ASCE/SEI 55-10 Tensile Membrane Structures
- ANSI/ASCE/EWRI 56-10 Guidelines for the Physical Security of Water Utilities
- ANSI/ASCE/EWRI 57-10 Guidelines for the Physical Security of Wastewater/Stormwater Utilities
- ASCE/T&DI/ICPI 58-10 Structural Design of Interlocking Concrete Pavement for Municipal Streets and Roadways
- ASCE/SEI 59-11 Blast Protection of Buildings
- ASCE/EWRI 60-12 Guideline for Development of Effective Water Sharing Agreements

FOREWORD

The Board of Direction approved revisions to the ASCE Rules for Standards Committees to govern the writing and maintenance of standards developed by ASCE. All such standards are developed by a consensus standards process managed by the ASCE Codes and Standards Committee (CSC). The consensus process includes balloting by a balanced standards committee and reviewing during a public comment period. All standards are updated or reaffirmed by the same process at intervals of five years.

This standard is a consolidation of the previous four-part *Automated People Mover Standards*. 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.

Chapters 1–11 cover requirements for design of an APM system, and Chapters 12–16 cover requirements for an APM in passenger operation, including chapters on security; emergency preparedness; system verification and demonstration; operations, maintenance, and training; and operational monitoring.

The standard also includes

- one mandatory annex on system safety program plan (SSPP) requirements;
- one nonmandatory reference bibliography of examples and guidance for other SSPPs;
- one nonmandatory informative annex on inspection and test guidelines; and
- two nonmandatory annexes: Recommended Practice for Acceptance of an APM System Application and Recommended Practice for Working Safely near APM Systems.

The provisions of the nonmandatory annexes and recommended practices are written in permissive language and, as such, offer the user a series of options or instructions, but do not prescribe a specific course of action. Significant judgment is left to the user of these annexes and recommended practices.

The development of these standards began in 1991 with a plan of producing partial standards in sequential segments. The first printing of Part 1, Chapters 1–6, was in 1996; followed by Part 2, Chapters 7 and 8, in 1998; Part 3, Chapters 9–11, in 2000; and the final Part 4, Chapters 1–6, in 2008.

During this early development period, Parts 1, 2, and 3 were reaffirmed on their five-year anniversary, as required by ASCE and ANSI rules and amended as needed.

The ultimate goal was to conduct a concurrent reaffirmation of all 16 chapters in one master volume to better serve the APM industry.

This publication now contains all 16 chapters of the completed standard and will be reaffirmed as needed, at least on a five-year cycle.

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

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

This standard will be beneficial to transportation engineers, civil engineers, safety engineers, and contractors of APM systems. Also, anyone who owns, operates, builds or maintains, designs, tests, insures, oversees, or certifies APMs or other innovative technology transit systems, such as magnetic levitation, air cushion, personal rapid transit, and monorail systems, will also benefit.

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 to warrant that the information contained herein is suitable for any general or specific use, and ASCE 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 his or her own responsibility.



Documents
Document Sharing Hub

This page intentionally left blank

10/04/2014 00:14:53 MDT



Documents
Document Sharing Hub

ACKNOWLEDGMENTS

The ASCE APM Standards Committee formed two decades ago as a volunteer group of individuals sharing a common belief that the fledgling APM industry would benefit by the development of a minimum set of requirements necessary to achieve an acceptable level of safety and performance for the public.

Many individuals and organizations from many backgrounds gave their time, resources and expertise in hosting meetings, providing web and email communications, drafting sections, and shepherding complicated technical specifications through the challenging consensus process and finally publication.

One individual stands out during these 22 years and is recognized by all committee members, past and present, as the driving force and catalyst behind the creation of this standard. This special acknowledgment is given to the founder and chairman of this committee for its first 17 years cumulating

with the final production of the four volume APM standard.

Tom McGean, Chairman Emeritus, has tirelessly led all aspects of the creation of the standard—from securing the sponsorship of ASCE, assembling a balanced membership from diverse backgrounds, nurturing the collegial spirit necessary to create a consensus standard, producing the standard in four consecutive parts to meet the evolving industry needs, and astutely guiding its acceptance within the competitive APM industry.

The committee dedicates this first publication of the combined standard to Tom McGean and hereby proclaims that this standard would not exist or be as well accepted by the transit and APM industry, without his quiet, persistent persuasion and gentle leadership.

Lawrence Smith, P.E., *Chair*; Paul Didrikson, P.Eng, *Secretary*; Tedd Snyder, P.E., *Vice-Chair*; Thomas McGean, P.E., *Past-Chair*

Abbas, Joseph D.
Ang, Michael G.
Baird, Douglas T.
Bares, Frank P.
Bondada, Murthy V. A.
Brackpool, Jon
Brunet, Pierre A.
Campbell, David B.
Champ, John J.
Clarissou, Yves F.
Clerc, Redjean
Cronin-North, Mary Catherine
Culver, Frank
De Leonardis, Peter
Deiparine, Michael
Didrikson, Paul
Dupre, Didier
Elms, Charles P.
Falvey, Robert W.
Fletcher, Jimmy E.

Frenz, Matthias
Friedmann, Darin
Friedreich, Ortfried
Fruehwirth, Alfred
Garcia, Antonio
Griebenow, Robert R.
Hartkorn, Albert W.
Hathaway, William T.
Hoelscher, James
Houts, Gary W.
Jensen, Kevin
Jussel, Dieter
Kapala, John
Lee, Jun-Ho
Leder, William H.
Lott, J. Sam
Lowson, Martin V.
Lynch, Stanford W.
May, Norman W.
McDermott, Patrick F.

McGean, Thomas J.
Mori, J. David
Morse, Diane I.
Muller, Peter J.
Nahke, Jorg
Poerschmann, Steven E.
Prell, Richard R.
Rettig, Thomas
Rhoton, Richard S.
Riseborough, Michael R.
Schrader Jr., Obe J.
Shumack, Michael
Smith, Lawrence
Snyder, Tedd L.
Spasopoulos, Pashalis
Thurston, David
Urien, Nicolas
Warner Jr., Ray
Weaver, Jack

This page intentionally left blank

.....



Documents
Document Sharing Hub

CONTENTS

Standards	iii
Foreword	v
Acknowledgments	vii
1 General	1
1.1 Scope	1
1.2 Existing Applications	1
1.3 New Applications	1
1.4 Reference Standards	1
1.5 Definitions	3
2 Operating Environment	7
2.1 Ambient Conditions	7
2.2 Induced Environmental Parameters	8
3 Safety Requirements	11
3.1 System Safety Program	11
3.2 Safety Principles	12
3.3 ATC System Fail-Safe Design	13
3.4 Verification and Validation	14
3.5 ATC System Mean Time Between Hazardous Events	15
3.6 Commentary on Chapter 3.0 and Subparts	15
4 System Dependability	17
4.1 Service Reliability	17
4.2 Service Maintainability	17
4.3 Service Availability	18
5 Automatic Train Control	19
5.1 Automatic Train Protection (ATP) Functions	19
5.2 Automatic Train Operation (ATO) Functions	22
5.3 Automatic Train Supervision (ATS) Functions	23
5.4 Manual Operation Limitations	25
6 Audio and Visual Communications	27
6.1 Audio Communication	27
6.2 Video Surveillance	28
6.3 Passenger Information Devices	28
7 Vehicles	31
7.1 Vehicle Capacity and Load	31
7.2 Vehicle Dynamic Envelope	31
7.3 Clearance in Stations	31
7.4 Vehicle Structural Design	32
7.5 Coupling	34
7.6 Suspension and Guidance	35
7.7 Passenger Comfort	35
7.8 Doors, Access, and Egress	38
7.9 Windows	38
7.10 Fire Protection and Flammability	38
7.11 Lighting	38
7.12 Electrical Systems	39



CONTENTS

8	Propulsion and Braking	41
8.1	Propulsion and Braking System Rating	41
8.2	Propulsion and Braking Methods	41
8.3	Braking Functions	41
8.4	Propulsion and Braking System Component Design	42
8.5	Installation and Protection	43
8.6	Controls and Interlocks	43
8.7	Brake Testing	43
9	Electrical Equipment	45
9.1	General	45
9.2	Traction Power Substation Equipment	46
9.3	Wayside Power Collection	47
9.4	Passenger Station Electrical Equipment	48
9.5	Uninterruptible Power Supply	48
10	Stations	51
10.1	Disabled Persons Access Requirements	51
10.2	Platform Edge Protection	51
10.3	Evacuation of Misaligned Trains	53
10.4	Emergency Lighting and Ventilation	53
10.5	Fire Protection	53
11	Guideways	55
11.1	Blue Light Stations	55
11.2	Intrusion Protection and Detection	55
11.3	Emergency Evacuation and Access	55
11.4	Fire Protection	56
11.5	Signage	56
11.6	Emergency Lighting and Ventilation	56
11.7	Emergency Power Supply	56
11.8	Guideway Alignment	56
11.9	Structural Criteria	57
12	Security	61
12.1	System Security Program	61
12.2	System Security Program Plan	61
13	Emergency Preparedness	63
13.1	Emergency Preparedness Program Plan	63
13.2	Training and Drills	64
13.3	Postemergency Incident and Drill Coordination	64
14	System Verification and Demonstration	65
14.1	Applicability of Prior Verification	65
14.2	Methods of Verification	65
14.3	System Verification Plan	65
14.4	Minimum Verification Requirements	66
14.5	Application-Specific Acceptance Requirements	67
15	Operations, Maintenance, and Training	75
15.1	System Operations Plan	75
15.2	Management Plan	75
15.3	Planned System Startup and Shutdown	75
15.4	Service Restoration Analysis	76
15.5	Alarms and Malfunctions Reporting	76

15.6	Recordkeeping and Management Reports	76
15.7	Maintenance	76
15.8	Training	77
16	Operational Monitoring	79
16.1	System Operational Monitoring Plan	79
16.2	Annual Internal Audit Responsibilities	79
16.3	Independent Audit Assessment	80
16.4	Inspections and Tests	81
16.5	Configuration Management	82
16.6	Interdepartmental and Interagency Coordination	82
16.7	Employee Safety Program	82
16.8	Hazardous Materials Program	82
16.9	Drug and Alcohol Abuse Program	82
16.10	Contractor Safety Coordination	82
16.11	Procurement	82
	Annex A. System Safety Program Requirements	83
	Annex B. Bibliography	89
	Annex C. Recommended Practice for Acceptance of an APM System Application	91
	Annex D. Inspection and Test Guidelines	93
	Annex E. Recommended Practice for Working Safely near APM Systems	97
	Index	101

This page intentionally left blank

.....



Documents
Document Sharing Hub

Chapter 1

GENERAL

1.1 SCOPE

This standard has been combined from four previous parts identified below, to expedite the approval and release process and to facilitate ease of use.

Previous Parts 1, 2, 3, and 4 of ASCE 21-05 and 21-08 cover a minimum set of requirements for design of an automated people mover (APM) with an acceptable level of safety and performance. The previous numbering system is retained (with additions):

Part 1 of ASCE 21-05 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 of ASCE 21-08 consists of

7. Vehicles
8. Propulsion and Braking

Part 3 of ASCE 21-08 consists of

9. Electrical Equipment
10. Stations
11. Guideways

Part 4 was a minimum set of requirements for maintaining an acceptable level of safety and performance for an automated people mover in passenger operation.

Part 4 of ASCE 21-08 consists of

12. Security
 13. Emergency Preparedness
 14. System Verification and Demonstration
 15. Operations, Maintenance, and Training
 16. Operational Monitoring
- Annex A. System Safety Program Requirements
Annex B. Bibliography
Annex C. Recommended Practice for Acceptance of an APM System Application
Annex D. Inspection and Test Guidelines
Annex E. Recommended Practice for Working Safely near APM Systems

1.2 EXISTING APPLICATIONS

Existing installations and projects in progress before 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:

AASHTO: American Association of State Highway and Transportation Officials, Suite 249, 444 North Capitol Street NW, Washington, D.C. 20001; phone (202) 624-5806.

AASHTO LRFD Bridge Design Specifications, 4th Edition, 2007 (cited in Sections 11.9.1, 11.9.2, and 11.9.3)

AASHTO Standard Specifications for Highway Bridges, 17th Edition, 2002 (cited in Sections 11.9.1, 11.9.2, and 11.9.3)

ACGIH: American Conference of Government Industrial Hygienists, 1330 Kemper Meadow Drive, Cincinnati, OH 45240; phone (513) 742-2020.

ACGIH Publication #7 DOC-648, *Whole Body Vibration: TLV Physical Agents*, 7th Edition, 2001, "Documentation" (cited in Section 7.7.3.2)

NOTE: An equivalent source for the above is ISO 2631-1-1985 (1985), *Evaluation of Human Exposure to Whole-Body Vibration*, which is no longer supported by or available from the ISO but may be purchased from the IHS Standards Store, 15 Inverness Way East, Englewood, Colo. 80112; phone (303) 792-2181 ext. 1950.



Documents
Document Sharing Hub

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

- ANSI S1.4-1983 (1983a), *Specification for Sound Level Meters* (cited in Sections 2.2.1 and 7.7.4)
- ANSI S3.29-1983 (1983b), *Guide to the Evaluation of Human Exposure to Vibration in Buildings* (cited in Section 2.2.2)
- ANSI/ASME B15.1-2000 (2000), *Safety Standard for Mechanical Power Transmission Apparatus* (cited in Section 8.5)
- ANSI B77.1-2006 (2006), *Passenger Ropeways—Aerial Tramways, Aerial Lifts, Surface Lifts, Tows and Conveyors—Safety Requirements* (cited in Sections 8.2.2 and 11.0)
- ANSI Z97.1-2004 (2004), *Safety Glazing Materials Used in Buildings—Safety Performance Specifications and Methods of Test* (cited in Sections 10.2.1 and 10.2.2)
- ANSI Z26.1-1996 (1996), *American National Standard, Safety Code for Safety Glazing Materials for Glazing Motor Vehicles Operating on Land Highways* (cited in Section 7.9)
- ANSI 117.1-2003 (2003), *Guidelines for Accessible and Usable Buildings and Facilities* (cited in Section 11.5)

APTA Publications: American Public Transportation Association, 1666 K Street, NW, Washington, D.C. 20006; phone (202) 496-4800.

APTA SS-E-010-98 (1998), *Standard for the Development of an Electromagnetic Compatibility Plan* (cited in Section 2.1.8)

ASHRAE: American Society of Heating, Refrigeration and Air Conditioning Engineers, 1791 Tullie Circle NE, Atlanta, Ga. 30329; phone (800) 527-4723.

2005 *ASHRAE Handbook Fundamentals Volume*, Chapter 28, Table 1 (cited in Section 7.7.1)

2009 *ASHRAE Handbook—Fundamentals*, Chapter 14, Climatic Design Information (cited in Section 2.1)

ASTM: Formerly the American Society for Testing and Materials, 100 Bar Harbor Drive, West Conshohocken, Penn. 19428-2959; phone (610) 832-9585.

ASTM D635-06 (2006a), *Standard Test Method for Rate of Burning and/or Extent and Time of Burning of Plastics in a Horizontal Position* (cited in Section 9.3.6)

ASTM C1036-06 (2006b), *Standard Specification for Flat Glass* (cited in Sections 10.2.1 and 10.2.2)

ASTM C1048-04 (2004), *Standard Specification for Heat Treated Flat Glass* (cited in Sections 10.2.1 and 10.2.2)

Code of Federal Regulations: U.S. Government Printing Office, Superintendent of Documents, 732 North Capitol Street, NW, Washington, D.C. 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)

16 CFR 1201, *Consumer Products Safety Commission Standard on Architectural Glazing Materials* (cited in Sections 10.2.1 and 10.2.2)

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

Weather of U.S. Cities, Fifth Edition, Vols. 1 and 2 (1996), by Richard A. Wood (cited in Section 2.1)

IEC Publications: International Electrotechnical Commission (IEC) Central Office, 3, rue de Varembe, CH-1211, Geneva 20, Switzerland; phone +41 22 919 02 11; Website: www.iec.ch.

IEC 62236 Edition 2.0, 2008–12, Parts 1–5, *Railway Applications—Electromagnetic Compatibility* (cited in Section 2.1.8)

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

IEEE Standard 1474.1-2004 (2004), *IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements* (cited in Sections 3.6 and 5.0)

IEEE Standard 32-1972 (1972, revised 1990), *Standard Requirements, Terminology and Test Procedures for Neutral Grounding Devices* (cited in Section 7.12.5)

IEEE Standard 242-2001 (2001), *Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems*, Section 1.0, First Principles (cited in Section 9.1.3)

IEEE Standard 519-1992 (1992), *IEEE Recommended Practices and Requirements for Harmonic Control in Electrical Power Systems* (cited in Section 9.2.3)

IEEE Standard 142-1991 (ANSI C114.1-1991) (1991), *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems* (cited in Section 9.1.4.1)

ISO: See ACGIH.

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

MIL-STD-810 F (2000), *Environmental Test Methods and Engineering Guidelines* (cited in Section 2.1.5)

NACE: National Association of Corrosion Engineers, 1440 South Creek Drive, Houston, Tex. 77084; phone (281) 228-6200.

NACE Standard RP0169-2002 (2002), *Control of External Corrosion on Underground or Submerged Metallic Piping Systems* (cited in Section 9.1.2)

NEMA: National Electrical Manufacturers Association, 1300 North 17th Street, Suite 1752, Arlington, Va. 22209; phone (703) 841-3200.

All NEMA standards (cited in Section 7.12.2.2)

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

NFPA 72-2002 (2002), *National Fire Alarm Code* (cited in Section 6.1.6)

NFPA 70, 2005 edition, *National Electrical Code* (cited in Sections 7.12.2.2, 9.1.4.2, 9.2.9, and 9.4)

NFPA 101, 2006 edition, *Life Safety Code* (cited in Section 10.4)

NFPA 130, 2003 and 2007 editions, *Fixed Guideway Transit and Passenger Rail Systems* (cited in Sections 6.1.2, 7.10, 7.10.1, 7.11.2, 7.12.2.1, 7.12.3, 9.1.1, 9.2.9, 10.4, 10.5.2, 10.5.3, 11.1, 11.3, 11.3.1, 11.3.2, 11.3.3, 11.4, 11.5, 11.6, and 11.7)

NOAA Publications: National Climatic Data Center, 151 Patton Avenue, Room 120, Asheville, N.C. 28801-0900; phone (828) 271-4800.

Local Climatologic Data, Annual Summary with Comparative Data, National Oceanic and Atmospheric Administration, updated annually (cited in Section 2.1)

SAE: Society of Automotive Engineers International, SAE World Headquarters, 400 Commonwealth Drive, Warrendale, Penn. 15096-0001; phone (877) 606-7323 (U.S. and Canada), 1-724-776-4970 (outside U.S. and Canada).

SAE J673-2005 (2005), *Automotive Safety Glasses* (cited in Section 7.9)

TIA, Telecommunications Industry Association Publications: Telecommunications Industry Association,

2500 Wilson Boulevard, Suite 300, Arlington, Va. 22201; phone (703) 907-7700.

Wireless Communications Systems—Performance in Noise and Interference-Limited Situations—Recommended Methods for Technology-Independent Modeling, Simulation, and Verification, Addendum 1, TIA/EIA Telecommunications Systems Bulletin TSB-88-A-1, January 2002 (cited in Section 6.1.6)

UL Publications: Underwriters Laboratories Publications, 333 Pfingsten Road, Northbrook, Ill. 60062; phone (847) 272-8800.

UL 96A, 11th Edition (2001), *Installation Requirements for Lightning Protection Systems* (cited in Section 2.1.4)

UL 813-1993 (1993), *Commercial Audio Equipment* (cited in Section 6.1.3)

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.

Bogie: The bogie consists of the elements that transmit lateral, longitudinal, and vertical loads between the guideway and the carbody. Bogies are also referred to as trucks.

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.

Carbody: The structural body shell, enclosing the passenger compartment(s).

Central Control: That 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.

Cosmetic Damage: Damage that does not impair system function, performance, safety, or structural integrity.

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 causes 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.

Guideway: A track or other riding surface (including supporting structure) that supports and physically guides transit vehicles specially designed to travel exclusively on it.

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 (Table 3-1).

Operating Loads: Definitions of operating loads are presented in Section 7.4.4.1.1 as lateral loads, vertical loads, and longitudinal loads.

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 that satisfactory operation of such is mandatory to mitigation of unacceptable and undesirable hazards as defined in 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.

Slow-Speed People Movers: Site applications in which all vehicles travel no more than 32 km/h (20 mph) at any location on their routes during normal operation.

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.

Tabletop Drill: A simulated or theoretical drill in which personnel carry out their functions by discussion.

Train: A train 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.



This page intentionally left blank

.....

Chapter 2

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

The following 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 and Atmospheric Administration (NOAA). Source number 2 summarizes the NOAA data in convenient form. Source number 3 provides temperature data and methods for calculating 50-year return temperatures specified in Section 2.1.1.

1. *Local Climatologic Data, Annual Summary with Comparative Data*, National Oceanic and Atmospheric Administration, updated annually.
2. *Weather of U.S. Cities*, Fifth Edition, Vols. 1 and 2, by Richard A. Wood, Gale Research Company, Detroit, MI, 1996; ISBN 0-8103-5525-6.
3. *2009 ASHRAE Handbook—Fundamentals*, Chapter 14, Climatic Design Information: ISBN: 978-1-933742-54-0; ISSN 1523-7222.

When the proposed site is located outside of the area of coverage of these documents or within a microclimate, data from these sources shall be augmented with local weather data.

2.1.1 Temperature and Humidity

The system shall be designed to, at a minimum, be capable of continuous operation and serviceability in site temperature conditions that represent the 50-year return highest maximum and lowest minimum extreme annual daily temperatures under naturally occurring combinations of temperature and humidity. Chapter 14, "Climatic Design Information," of ASHRAE (2009) demonstrates the method of calculating the 50-year return temperatures. Also, it is not

intended that the automated people mover (APM) system should operate when the service area (e.g., urban area or major activity center) is closed because of any of these extreme conditions.

The temperature and relative humidity limit requirements for equipment shall reflect the operating environment at the location in the system where it is installed. These environmental conditions are not intended for the design and operation of the HVAC systems.

2.1.2 Wind

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

1. Normal system operation,
2. Manual operation, and
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. Historical data are defined as the extreme conditions under which the area to be served (e.g., urban area or major activity center) would remain in operation and not be closed. It is not intended to impose operational requirements more restrictive than the owner intends.

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 UL 96A, 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 Military Standard MIL-STD-810-F (2000), 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 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 of the International Electrotechnical Commission (IEC) 62236 series of standards, in particular,

- IEC 62236-1, *Railway Applications—Electromagnetic Compatibility—Part 1: General*
- IEC 62236-2, *Railway Applications—Electromagnetic Compatibility—Part 2: Emission of the Whole Railway System to the Outside World*
- IEC 62236-3-1, *Railway Applications—Electromagnetic Compatibility—Part 3-1: Rolling Stock—Train and Complete Vehicle*

- IEC 62236-3-2, *Railway Applications—Electromagnetic Compatibility—Part 3-2: Rolling Stock—Apparatus*
- IEC 62236-4, *Railway Applications—Electromagnetic Compatibility—Part 4: Emission and Immunity of the Signalling and Telecommunications Apparatus*
- IEC 62236-5, *Railway Applications—Electromagnetic Compatibility—Part 5: Emission and Immunity of Fixed Power Supply Installations and Apparatus*

An electromagnetic compatibility (EMC) control plan and/or EMC management plan shall be developed in accordance with APTA SS-E-010-98 (1998).

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 ANSI Standard S1.4-1983 (1983a), and shall be set for fast or slow response as indicated.

1. Vehicle stopped on the guideway in a free field with all auxiliary onboard equipment in normal operation at a point outside, 1.5 m (5 ft) from the doorway on a line aligned to the centerline of the doorway and perpendicular to the plane of the doorway and 1.5 m (5 ft) above the doorway threshold: 74 dB (slow response).
2. Under all normal operating conditions in a free field, 15 m (50 ft) from guideway centerline and 1.5 m (5 ft) above ground level to 1.5 m (5 ft) above guideway running surface: 76 dB (fast response).
3. For the purposes of measurement, the “free field” is approximated in tests carried out in an open area away from any major obstructions or noise reflectors.

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 dB level.

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

2.2.1.1 Commentary for Interior Noise Levels (Section 7.7.4) and Exterior Airborne Noise (Section 2.2.1) Limits in Tunnels

The following commentary is provided as an explanation of why the standard does not specify noise limits inside buildings and tunnels.

The conditions for measuring vehicle exterior airborne noise are specified in Section 2.2.1 as, “Under all normal operating conditions *in a free field*, 15 m (50 ft) from guideway centerline and 1.5 m (5 ft) above ground level to 1.5 m (5 ft) above guideway running surface.”

The conditions for measuring vehicle interior noise is specified in Section 7.7.4 as “. . . with all auxiliary equipment operating. All noise measurements are to be taken *in a free field environment*, with no passengers (up to three test personnel permitted) in the vehicle. Interior noise levels shall be measured 1.5 m (5 ft) above the floor, above the suspension and/or running gear, and at the geometric center of the vehicle floor . . .”

In both cases, the vehicle is specified to be operating in a *free field environment* to determine purely the noise energy that is emitted from the train without any content of reflected noise or other noise generators that otherwise can compromise the measurements.

When a vehicle or train is operated inside a tunnel or building, noise emitted from the vehicle or train can be reflected and can increase the amplitude of the measured noise. Because the geometries,

designs, and surface materials of such structures can vary significantly, it is not possible to know the extent that reflected noise may be experienced. Hence, neither consistent conditions nor standard tests exist for specifying noise limits in tunnels and buildings.

The current standard sets a limit on the noise energy that can be emitted by a vehicle or train. Designers of buildings and tunnels are provided with the limit on emitted noise energy that they need as an input on which they can make designs. Because they are in control of the architectural structure (size, shape, materials, and reflective surfaces), they are in control of what the resultant noise is in a tunnel or building. Buyers of APM systems can specify noise limits, taking into account the architectural designs they specify.

2.2.2 Structure-Borne Noise and Vibration

System-induced vibrations shall be imperceptible at or in surrounding buildings. The threshold of perception shall be as defined by ANSI Standard S3.29-1983 (1983b).

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, Subparts S and T, and the interference requirements defined in Title 47, Chapter I, Part 15.

This page intentionally left blank

Chapter 3

SAFETY REQUIREMENTS

A system safety program, per Section 3.1, shall be instituted during the system planning and design phase and shall 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 (SSPP) to assist in implementing and documenting that program. The SSPP shall identify the responsibilities of all parties for implementing a system safety program.

The system safety program and SSPP shall

1. Have as their objective to provide for the safety of the passengers, employees, the 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; and
6. Provide for and maintain owner and 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 ensure its implementation and shall report directly to top management.

3.1.1 System Safety Program Plan

An SSPP shall be developed during the planning and design phase of the APM project and shall be maintained current throughout the APM system life cycle. The SSPP shall be prepared in general accordance with Annex A, System Safety Program Require-

ments, A.1 (System Safety Program Plan), or the equivalent. The SSPP shall, at 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 the following:

1. Data from previous accidents or operating experience;
2. Expert opinion and hazard scenarios;
3. Checklists of potential hazards;
4. Previous hazard analyses; and
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 (Table 3-1) based on mean time between hazardous events (MTBHE) 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 used, 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; and
7. Eliminate the system, subsystem, or 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

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

Notes:

IA, IIA, IIIA, IB, IIB, and IC = Unacceptable.

ID, IIC, and IIIB = Undesirable (allowable with agreement from authority having jurisdiction).

IE, IID, IIE, IIIC, IIID, IVA, and IVB = Acceptable with notification to the authority having jurisdiction.

IIIE, IVC, IVD, and 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 subjectively 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.

shall be conducted to identify and resolve any new hazards.

3.1.2.1 Hazard Analyses

Hazard analyses shall be used 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 sub-system 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 the equivalent, respectively.

3.2 SAFETY PRINCIPLES

The following safety principles shall be observed in the APM system (Table 3-1 defines 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 (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 implement these activities adequately shall also be identified.

3.3 ATC SYSTEM FAIL-SAFE DESIGN

All safety-critical elements of the ATC system (see Chapter 5, Automatic Train Control) shall be designed and implemented in accordance with fail-safe principles and shall use one or more of the techniques described as follows, or the 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 mode and effects analysis, or the equivalent.

3.3.2 Alternatives to Intrinsic Fail-Safe Design

Many control system designs use 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 (Sections 3.3.2.1 through 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 be its ability to detect fault conditions and ensure 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 ensure 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 with all 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 one another so that no common environmental or power fluctuations, errors, and/or faults can cause unacceptable or undesirable hazards (Table 3-1).
5. The checking process shall be comprehensive in coverage (including 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 (Table 3-1).
6. For units using software-programmed elements, the software shall be shown to be free from errors, including any errors introduced during the compilation process, by proven principles and 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 or teams, using different languages and tools. The hardware may or may not be identical, or it 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 with all 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 one another so that no common environmental or power fluctuations, errors, and/or faults can cause unacceptable or undesirable hazards (Table 3-1).
5. The checking process shall be comprehensive in coverage (including 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 (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 with the diverse checking process or with 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 (including 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 (Table 3-1).
5. For units using software-programmed elements, the software shall be shown to be free from errors, including any errors introduced by the compilation process by proven principles or 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 the previous characteristic, 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 (including 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 (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 process includes elements designed and implemented in accordance with safety principles (Section 3.2) and ATC 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 on which the assurance of safety depends. Such factors shall be directly associated with the design concept used, i.e., 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.

3.5 ATC SYSTEM MEAN TIME BETWEEN HAZARDOUS EVENTS

The ATC system (see Chapter 5, Automatic Train Control) shall, in addition to the aforementioned, have a calculated aggregate mean time between hazardous events (MTBHE) (total of all catastrophic and critical hazards) of $10^{*}8$ ($1 \times E 8$) system operating hours or greater. System safety documentation shall support this aggregate MTBHE calculation and substantiate the methodology used to arrive at the result.

3.6 COMMENTARY ON CHAPTER 3.0 AND SUBPARTS

Section 3.4 of this standard describes formal procedures for verifying and validating that safety-critical hazards have been identified and resolved. It should be noted that Section 3.4 does not apply just to the ATC system but rather requires verification and validation of *all* safety-critical hardware and software elements of the entire APM system that were identified in the hazard resolution process explained in Section 3.1.2 of the standard.

Unlike Section 3.4, Section 3.5 provides an additional MTBHE requirement that applies *only* to the ATC system.

As noted in Section 3.1.2, all individual APM system or subsystem hazards are to be assessed in terms of both the severity and consequence of the hazard and its likelihood of occurring. The risk assessment table (Table 3-1) provided in the standard is to be used as a basis for deciding whether the hazard needs to be eliminated or mitigated or whether it may be accepted. The table provides guidelines for the level of risk that is completely acceptable, the level allowable provided notice is given to the authority having jurisdiction, and the level that can only be accepted with the specific approval of the authority having jurisdiction. Finally, there is a risk level that is so serious that it cannot be accepted and must be either mitigated or eliminated.

It is important to emphasize that this evaluation is performed on each individually identified system or subsystem hazard for the entire APM system. As noted in Table 3-1, it is understood that quantifiable estimates of probability or frequency of occurrence

may not always be available. In that event, it is acceptable to subjectively or qualitatively estimate the risk. If such qualitative estimates are used, all subjectively determined elements are to be identified and the rational justification for the estimate is to be documented.

The results of this process would normally be a set of hazard resolution forms describing each hazard, the consequence of the hazard and its severity, and the steps taken to mitigate or eliminate the hazard if it is not acceptable. The form also documents the residual acceptable risk level after mitigation in the event the hazard has not been completely eliminated.

Section 3.1.2 of the standard lists acceptable approaches to elimination or mitigation of hazards. The preferred solution is to eliminate or control the hazard by a design change. If this solution is not possible, safety or warning devices can be used. If this solution is not practicable, procedures such as periodic inspection are suggested. Finally, the offending equipment responsible for introducing the hazard can simply be eliminated from the design altogether. Acceptance of the hazard is only allowed if it is not in one of the shaded risk categories in Table 3-1. These shaded risk areas represent an unacceptable combination of hazard severity and likelihood of occurrence.

Section 3.5 sets an additional safety criterion for the ATC system over and above the mitigation or elimination of individual hazards required by Section 3.4. This additional safety criterion is an aggregate MTBHE (total of all catastrophic and critical hazards) for just the ATC system. This MTBHE figure is to be supported by safety documentation.

Two different overall MTBHE values are specified. If the system does not use communications-based train control (CBTC), the requirement is a calculated aggregate MTBHE of $10^{*}8$ system operating hours or greater for the entire ATC system.

If the ATC system uses CBTC, the MTBHE requirement is to be superseded by that specified in IEEE 1474.1-2004 (2004), Section 5.3.4. This section specifies an MTBHE of a least $10^{*}9$ operating hours for all wayside and train-borne CBTC equipment in a contiguous portion of a one-way route that can be traversed by a train traveling at the specified maximum authorized speed for one hour or less. In addition, the maximum number of trains should be in operation on the segment at their peak operating headway.

It should be noted that the $10^{*}8$ number in this standard covers the entire ATC system, whereas the $10^{*}9$ number covers only car and wayside CBTC equipment on only a portion of the total route, so the two numbers are not directly comparable.

This page intentionally left blank

Chapter 4

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 chapter.

Throughout this chapter, references to “system” may also be applied to “system subsets” for purposes of determining their individual contribution to overall system dependability.

Partial service or degraded service adjustments may be applied in defining overall system dependability. Factors, ratios, or 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 failures ($MTBF_s$).

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

where

OH_s = Total number of hours of scheduled operation over which the service reliability is being determined; the period of operating hours, and

NF_s = Number of failures, malfunctions, and operating disruptions classified as service interruptions during the period of operating hours.

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 caused by 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, and
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 caused by 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 caused by 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; and
6. Stoppages caused by 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 ($MTTR_s$) after a system service interruption.

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

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

where

TTR_i = Time to restore service after the i th service interruption (downtime interval), and

NF_s = Number of failures, malfunctions, and operating disruptions classified as service interruptions during the period of operating hours.

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 4.1.2) 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 or 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.

Chapter 5

AUTOMATIC TRAIN CONTROL

The 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 automated people mover (APM) systems that use communications-based train control (CBTC) for ATC, the requirements of IEEE 1474.1-2004 (2004) shall apply in lieu of the requirements provided in Sections 5.1 and 5.2.

5.1 AUTOMATIC TRAIN PROTECTION (ATP) FUNCTIONS

All ATP functions shall be designed and implemented in accordance with Sections 3.2, Safety Principles, and 3.3, ATC System Fail-Safe Design.

5.1.1 Presence Detection

Presence detection shall be an ATP function if it is required to ensure 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 shall be located and identified by positive detection before the resumption of automatic operation. In no case shall automatic operation be allowed based on 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 requirement 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 and traction, and
8. Maximum design tailwind.

For stopping distance calculation purposes, minimum emergency braking condition shall be based on 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 use 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, ATC 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, 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 or detached train and all other trains connected to that mechanism.

Comparable separation assurance protection shall be required for APM systems that use 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 that 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 close 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 the 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.

5.1.6 Parted Consist Protection

Parted consist protection shall be an ATP function for APM systems that use 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 separated entity 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 m/s (0.95 ft/s) 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 (of a train or station), a local manual reset by authorized personnel shall be required before 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 before 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, and
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 m/s (1.1 ft/s).
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.

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 Chapter 5, 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 or 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 ensure 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 used 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 used 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 percent 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 caused by momentary loss of power or train detection shall be provided.

5.1.15 Off-Line Sections Operation—Special Conditions

Off-line sections are defined as guideway sections featuring automatic operation at restricted speed, such as off-line stations or vehicle storage areas (lanes). For off-line sections operation, three different zones are considered:

1. Transition zone to and from the main line,
2. Circulation zone, and
3. Docking zone.

Transition zone: When entering or leaving the main line to or from the off-line section, the vehicle shall be detected by the ATP system of the off-line section, and speed shall be adjusted accordingly. Vehicle movement between main-line and off-line lanes shall be accomplished in accordance with the principles of Section 5.1.14.

Circulation zone: Contact between two moving vehicles may be acceptable at low speed, only under failure conditions, if the contact speed is low enough as determined by an analysis conducted in accordance with Section 3.1.2.1, Hazards Analyses, to

1. protect against damage to vehicles (reversible shock absorbers may be used) and
2. protect against passenger injuries (collision impact shall meet all criteria of Section 7.4.4.9.2).

The permissible contact speed shall be enforced by ATP.

Docking zone: Contact between a moving vehicle and a vehicle stopped at a docking position (with doors open and brakes applied as per Section 5.1.8) may be acceptable at low speed, only under failure conditions, if the contact speed is low enough, as determined by an analysis conducted in accordance with Section 3.1.2.1, Hazards Analyses, to

1. protect against damage to vehicles (reversible shock absorbers may be used);
2. protect against passenger injuries (collision impact shall meet all criteria of Section 7.4.4.9.2); and
3. prevent any movement of the stopped vehicle. Passenger on platform and passenger embarking and disembarking safety shall be in accordance with Section 10.2, Platform Edge Protection. Door control protection and departure interlocks shall be in accordance with Sections 5.1.10 and 5.1.11, respectively.

5.2 AUTOMATIC TRAIN OPERATION (ATO) FUNCTIONS

The ATO shall function to automatically operate trains around 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 over-speed 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-in.) 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 (of the train or 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 (ATS) FUNCTIONS

Automatic train supervision (ATS) 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 a central control office, 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 ATS

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, and
2. All propulsion power shuts 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 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,