IEEE Std 1474.1™-2004
(Revision of
IEEE Std 1474.1-1999)

IEEE Standards

1474.1™

IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements

IEEE Vehicular Technology Society

Sponsored by the
Rail Transit Vehicle Interface Standards Committee

IEEE

3 Park Avenue, New York, NY 10016-5997, USA

25 February 2005

Print: SH95275
PDF: SS95275

Recognized as an
American National Standard (ANSI)

IEEE Std 1474.1™-2004(R2009)
(Revision of
IEEE Std 1474.1-1999)

IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements

Sponsor

Rail Transit Vehicle Interface Standards Committee
of the
IEEE Vehicular Technology Society

Approved 1 February 2005

American National Standards Institute

Reaffirmed 11 September 2009
Approved 23 September 2004

IEEE-SA Standards Board

Abstract: Performance and functional requirements for a communications-based train control (CBTC) system are established in this standard. A CBTC system is a continuous, automatic train control system utilizing high-resolution train location determination, independent of track circuits; continuous, high-capacity, bidirectional train-to-wayside data communications; and train-borne and wayside processors capable of implementing automatic train protection (ATP) functions, as well as optional automatic train operation (ATO) and automatic train supervision (ATS) functions. In addition to CBTC functional requirements, this standard also defines headway criteria, system safety criteria, and system availability criteria for a CBTC system. This standard is applicable to the full range of transit applications including automated people movers.
Keywords: automation, communications, signaling, train control

---

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Print: ISBN 0-7381-4486-X SH95275
PDF: ISBN 0-7381-4487-8 SS95275

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854

USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

[This introduction is not part of IEEE Std 1474.1-2004, IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.]

This introduction provides some background on the rationale used to develop this standard. This information is meant to aid in the understanding, usage, and applicability of this standard.

Conventional signaling/train control systems rely almost exclusively on track circuits to detect the presence of trains. Information on the status of the track ahead is provided to train operators either through wayside signals or train-borne cab signals. Ensuring compliance with the signals is achieved through operating procedures, wayside automatic train stops, or train-borne supervisory equipment linked to the train's braking system. These conventional systems are effective in providing train protection, but are not particularly efficient in maximizing the utilization of the rail transit infrastructure, as a result of a number of fundamental limitations, specifically, the following:

a) The location of trains can only be determined to the resolution of the track circuits; if any part of a track circuit is occupied by a train, the whole track circuit must be assumed to be occupied by the train. Track circuits can be made shorter, but each additional track circuit requires additional wayside hardware, so there is an economical and practical limit to the number of track circuits that can be provided.

b) The information that can be provided to a train is limited to a small number of wayside signal aspects or a small number of speed codes in a cab signal system.

c) For a wayside signal system with automatic train stops but without continuous cab signaling, enforcement is intermittent.

CBTC systems overcome these fundamental limitations of conventional track circuit-based systems, and therefore, permit more effective utilization of the transit infrastructure. This is accomplished, for example, by allowing trains to operate safely at much closer headways, by permitting greater flexibility and greater precision in train control, and by providing continuous safe train separation assurance and overspeed protection. Additional benefits of CBTC technology include the economical support of automatic train operations (both on the mainline and in maintenance yards), improved reliability, and reductions in maintenance costs through a reduction in wayside equipment and real-time diagnostic information. The basic characteristics of a CBTC system include the following:

1) Determination of train location, to a high degree of precision, independent of track circuits.

2) A geographically continuous train-to-wayside and wayside-to-train data communications network to permit the transfer of significantly more control and status information than is possible with conventional systems.

3) Wayside and train-borne vital processors to process the train status and control data and provide continuous automatic train protection (ATP). Automatic train operation (ATO) and automatic train supervision (ATS) functions can also be provided, as required by the particular application.

Although the benefits of CBTC technology are recognized, there are currently no independent standards defining the performance and functional requirements that need to be satisfied by CBTC systems in order to realize enhanced performance, availability, train operational flexibility, and train protection. This standard has been developed to address this.

Notice to users

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

At the time this standard was completed, the Communications-Based Train Control Working Group had the following membership:

Alan F. Rumsey, *Chair*

George Achakji
Stephane Bois
Corinne Braban
Frederick Childs
Michael Crispo
Nicolas Estivals
Harold Gillen
Harvey Glickenstein
Vic Graponne
James Hoelsher
Geoff Hubbs
Kenneth A. Karg
John LaForce
Martin Lukes
Dave Male
Charles Martin
Norman. May
Bob Miller
William Petit
Venkat Pindiprolu
Carl Schwellnus
Mickey Senase
Errol Taylor
John Vogler
Ken Vought
Robert E. Walsh
David Zahorsky

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Corinne Braban
Frederick Childs
Michael Crispo
David Dimmer
Jeff Eilenberg
Nicolas Estivals
Harvey Glickenstein
James Hoelsher
Geoff Hubbs
Kenneth A. Karg
John LaForce
Martin Lukes
Charles Martin
Norman May
Tom McGean
William Petit
Venkat Pindiprolu
Alan F. Rumsey
Louis Sanders
Jeffrey Smith
John Vogler
Robert E. Walsh

When the IEEE-SA Standards Board approved this standard on 23 September 2004, it had the following membership:

Don Wright, *Chair*
Steve M. Mills, *Vice Chair*
Judith Gorman, *Secretary*

Chuck Adams
Stephen Berger
Mark D. Bowman
Joseph A. Bruder
Bob Davis
Roberto de Marca Boisson
Julian Forster*
Arnold M. Greenspan
Mark S. Halpin
Raymond Hapeman
Richard J. Holleman
Richard H. Hulett
Lowell G. Johnson
Joseph L. Koepfinger*
Hermann Koch
Thomas J. McGean
Daleep C. Mohla
Paul Nikolich
T. W. Olsen
Ronald C. Petersen
Gary S. Robinson
Frank Stone
Malcolm V. Thaden
Doug Topping
Joe D. Watson

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Richard DeBlasio, *DOE Representative*
Alan Cookson, *NIST Representative*

Don Messina
IEEE Standards Project Editor

Contents

IEEE Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements

1. Overview

This standard establishes performance and functional requirements for a CBTC system. It is divided into six clauses. Clause 1 describes the scope and purpose of this standard. Clause 2 lists references that are useful in applying this standard. Clause 3 provides definitions that are either not found in other standards or have been modified for use with this standard. Clause 4 defines the general operating requirements for CBTC systems, including train operating modes to be supported. Clause 5 defines the performance requirements for CBTC systems, including headway criteria, system safety criteria, and system availability criteria. Clause 6 defines the functional requirements for CBTC systems, including automatic train protection (ATP) functions, automatic train operation (ATO) functions, and automatic train supervision (ATS) functions.

1.1 Scope

This standard establishes a set of performance and functional requirements necessary for enhancing performance, availability, operations, and train protection using a CBTC system.

1.2 Purpose

There are currently no independent standards defining the performance and functional requirements to be satisfied by CBTC systems. This standard will enhance performance, availability, operations, and train protection and will facilitate new CBTC applications.

1.3 Existing applications

Existing CBTC installations and projects in progress prior to the publication of this standard need not comply with the new or revised requirements of this standard, IEEE Std 1474.1-2004, except where specifically required by the authority having jurisdiction.

2. Normative references

This standard shall be used in conjunction with the following publications. In case of a conflict between this standard and the referenced document, this standard shall take precedence. Those provisions of the referenced documents that are not in conflict with this standard shall apply as referenced.

IEEE Std 1474.2™-2003, IEEE Standard for User Interface Requirements in Communications-Based Train Control (CBTC) Systems.[1,2]

IEEE Std 1475™-1999, IEEE Standard for the Functioning of and Interfaces Among Propulsion, Friction Brake and Train-borne Master Control on Rail Rapid Transit Vehicles.

IEEE Std 1477™-1998 (Reaff 2003), IEEE Standard for Passenger Information System for Rail Transit Vehicles.

IEEE Std 1478™-2001, IEEE Standard for Environmental Conditions for Transit Rail Car Electronic Equipment.

IEEE Std 1483™-2000, IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

IEEE Std 1570™-2002, IEEE Standard for the Interface Between the Rail Subsystem and the Highway Subsystem at a Highway Rail Intersection.

IEEE P1582™ (Draft 1.0, February 2002), Draft Standard for Environmental Requirements for Rail Transit Automatic Train Control Systems Wayside Equipment.[3]

3. Abbreviations, acronyms, and definitions

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition [B4][4], should be referenced for terms not defined in this clause.

3.1.1 authority having jurisdiction: The entity that defines the contractual (including specification) requirements for the procurement.

3.1.2 automated people movers (APMs): A guided transit mode with fully automated operations, featuring vehicles that operate on guideways with exclusive right-of-way.

3.1.3 automatic train control (ATC): The system for automatically controlling train movement, enforcing train safety, and directing train operations. ATC must include ATP and may include ATO and/or ATS.

---

[1]The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[3]This IEEE standards project was not approved by the IEEE-SA Standards Board at the time this publication went to press. For information about obtaining a draft, contact the IEEE.

[4]The numbers in brackets correspond to those of the bibliography in Annex A.

3.1.4 automatic train operation (ATO): The subsystem within the ATC system that performs any or all of the functions of speed regulation, programmed stopping, door control, performance level regulation, or other functions otherwise assigned to the train operator.

3.1.5 automatic train protection (ATP): The subsystem within the ATC system that maintains fail-safe protection against collisions, excessive speed, and other hazardous conditions through a combination of train detection, train separation, and interlocking.

3.1.6 automatic train supervision (ATS): The subsystem within the ATC system that monitors trains, adjusts the performance of individual trains to maintain schedules, and provides data to adjust service to minimize inconveniences otherwise caused by irregularities.

NOTE—The ATS subsystem also typically includes manual and automatic routing functions.[5]

3.1.7 auxiliary wayside system: A back-up or secondary train control system, capable of providing full or partial ATP for trains not equipped with train-borne CBTC equipment and/or trains with partially or totally inoperative train-borne CBTC equipment. The auxiliary wayside system may include train-borne equipment and may also provide broken rail detection.

3.1.8 basic operating unit: (A) A single vehicle designed for independent operation. **(B)** A permanent or semi-permanent combination, designed for independent operation, consisting of two or more vehicles of one or more types.

3.1.9 brake, emergency: Fail-safe, open-loop braking to a complete stop, with an assured maximum stopping distance considering all relevant factors. Once the brake application is initiated, it is irretrievable (i.e., it cannot be released until the train has stopped or a predefined time has passed).

3.1.10 brake, (maximum) service: A non-emergency brake application that obtains the (maximum) brake rate that is consistent with the design of the brake system, retrievable under the control of master control.

3.1.11 car: *See:* **vehicle.**

3.1.12 civil speed limit: The maximum speed authorized for each section of track, as determined primarily by the alignment, profile, and structure.

3.1.13 communications-based train control (CBTC): A continuous ATC system utilizing high-resolution train location determination, independent of track circuits; continuous, high capacity, bidirectional train-to-wayside data communications; and train-borne and wayside processors capable of implementing vital functions.

3.1.14 commuter rail: A passenger railroad service that operates within metropolitan areas on trackage that usually is part of the general railroad system. The operations, primarily for commuters, are generally run as part of a regional system that is publicly owned or by a railroad company as part of its overall service.

3.1.15 consist: The makeup or composition (number and specific identity) of individual units of a train.

3.1.16 dwell time: The time a transit unit (vehicle or train) spends at a station or stop, measured as the interval between its stopping and starting.

3.1.17 fail-safe: A design philosophy applied to safety-critical systems such that the result of hardware failure or the effect of software error shall either prohibit the system from assuming or maintaining an unsafe state or shall cause the system to assume a state known to be safe.

[5]Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

3.1.18 headway: The time interval between the passing of the front ends of successive vehicles or trains moving along the same lane or track in the same direction.

3.1.19 heavy rail transit: A mode of rail rapid transit generally characterized by fully grade-separated construction, operating on exclusive rights-of-way and station platforms at the floor level of the vehicles.

3.1.20 interlocking: An arrangement of switch, lock, and signal devices that is located where rail tracks cross, join, separate, and so on. The devices are interconnected in such a way that their movements must succeed each other in a predefined order, thereby preventing opposing or conflicting train movements.

3.1.21 light rail transit: A mode of rail transit characterized by its ability to operate on exclusive rights-of-way, street running, center reservation running, and grade crossings, and to board and discharge passengers at track or vehicle floor level.

3.1.22 master control: The train-borne device or system directly providing the control signals to the train.

3.1.23 movement authority: The authority for a train to enter and travel through a specific section of track, in a given travel direction. Movement authorities are assigned, supervised, and enforced by a CBTC system to maintain safe train separation and to provide protection through interlockings.

3.1.24 redundancy: The existence in a system of more than one means of accomplishing a given function.

3.1.25 reliability: The probability that a system will perform its intended functions without failure, within design parameters, under specific operating conditions, and for a specific period of time.

3.1.26 safe braking model: An analytical representation of a train's performance while decelerating to a complete stop, allowing for a combination of worst-case influencing factors and failure scenarios. A CBTC-equipped train will stop in a distance equal to or less than that guaranteed by the safe braking model.

3.1.27 safety critical: (A) A term applied to a system or function, the correct performance of which is critical to safety of personnel and/or equipment. **(B)** A term applied to a system or function, the incorrect performance of which may result in a hazard.

NOTE—Vital functions are a subset of safety-critical functions.

3.1.28 self-revealing failure: Failures whose effects on system operation are immediately and clearly apparent.

3.1.29 service, revenue: (A) Transit service excluding deadheading or layovers. **(B)** Any service scheduled for passenger trips.

3.1.30 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.

3.1.31 System Safety Program: The combined tasks and activities of system safety management and system safety engineering that enhance operational effectiveness by satisfying the system safety requirements in a timely, cost-effective manner throughout the system life cycle.

3.1.32 train: A consist of one or more basic operating units.

3.1.33 unit: *See:* **basic operating unit.**

3.1.34 vehicle: A land conveyance assembly for carrying or transporting people and objects capable of traversing a guideway, having structural integrity and general mechanical completeness, but not necessarily designed for independent operation.

3.1.35 vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.

3.2 Abbreviations and acronyms

APM	automated people mover
APTA	American Public Transportation Association
AREMA	American Railway Engineering and Maintenance-of-Way Association
ASCE	American Society of Civil Engineers
ATC	automatic train control
ATO	automatic train operation
ATP	automatic train protection
ATS	automatic train supervision
CBTC	communications-based train control
GEBR	guaranteed emergency brake rate
MTBF	mean time between failure
MTBFF	mean time between functional failure
MTBHE	mean time between hazardous event
MTTR	mean time to repair
MTTRS	mean time to restore service
O&SHA	operating and support hazard analysis
PHA	preliminary hazard analysis
SHA	system hazard analysis
SSHA	subsystem hazard analysis
SSPP	System Safety Program Plan

4. General requirements

4.1 Characteristics of CBTC systems

The primary characteristics of a CBTC system include the following:

a) High-resolution train location determination, independent of track circuits

b) Continuous, high capacity, bidirectional train-to-wayside data communications

c) Train-borne and wayside processors performing vital functions

4.2 Categorization of CBTC systems

This standard recognizes that different configurations of CBTC systems are possible, depending on the specific application. For example, a CBTC system may

a) Provide ATP functions only, with no ATO or ATS functions.

b) Provide ATP functions, as well as certain ATO and/or ATS functions, as required to satisfy the operational needs of the specific application.

c) Be the only train control system in a given application or may be used in conjunction with other auxiliary wayside systems.

A typical functional block diagram for a CBTC system is given in Annex B.

4.3 Range of applications

The CBTC performance and functional requirements defined in this standard are intended to be applicable to the full range of transit applications, including light rail, heavy rail, and commuter rail transit systems, and shall be applicable to other transit applications, such as automated people movers (APMs) if CBTC is used for ATC.

NOTE—ASCE 21-96 [B3] establishes additional requirements related to operating environment, safety requirements, system dependability, and audio/visual communications for APM systems.

It is the intent of this standard that tiered levels of functionality, and interoperability between equipment provided by multiple vendors, are facilitated to the extent required by the authority having jurisdiction. All CBTC systems shall include ATP functions.

4.4 Train configurations

A CBTC system shall be capable of supporting a variety of train configurations, including the following:

a) Fixed-length unidirectional trains comprised of one or more basic operating units

b) Fixed-length bidirectional trains comprised of one or more basic operating units

c) Variable-length unidirectional trains

d) Variable-length bidirectional trains

A CBTC system shall be capable of supporting a mixed fleet of trains, where specific trains, and/or classes of trains, have different performance characteristics.

4.5 Train operating modes

CBTC-equipped trains may be operated by either a single person or a multi-person crew. A CBTC system may also be required to support operation of trains without crews.

For operation of trains with crews, the train operator will typically be stationed in the lead car of the train and will be responsible for moving the train from station to station. With a multi-person crew, the conductor(s) will normally operate from conductor position(s) within the train to operate the train's doors. A CBTC system shall support single-person train operation by combining the conductor and train operator display information on the train operator's display. For multi-person crews, conductor display information shall also be provided on separate conductor displays.

For the purposes of this standard, operation of trains without crews includes both unattended and driverless train operations. With unattended train operations, there would normally be no crew member onboard the train. With driverless train operations, there may be a crew member onboard the train, but normally not in the driving cab. This crew member, if present, would normally have no responsibility for operation of the train except for failure recovery.

CBTC-equipped trains (including CBTC-equipped maintenance vehicles) shall be capable of operating in various modes, depending on whether the train is operating in CBTC territory or non-CBTC territory, and depending on the operational status of the train-borne and/or wayside CBTC equipment.

Mixed-mode operation shall also be considered a normal operating mode, to the extent specified by the authority having jurisdiction. Mixed-mode operation is defined as the simultaneous operation within CBTC territory of CBTC-equipped trains and trains that are not equipped with functional train-borne CBTC equipment (including maintenance vehicles). Mixed-mode operation may be used in one or more of the following ways:

a) A regularly scheduled mode of operation within CBTC territory
b) An infrequent, unscheduled mode of operation within CBTC territory
c) During the transition period only, as a new CBTC system is cut-in
d) As a result of train-borne CBTC equipment failures

4.5.1 Normal train operating modes in CBTC territory

4.5.1.1 CBTC-equipped trains

CBTC-equipped trains operating in CBTC territory shall operate, within ATP limits, under the protection of the CBTC system. The train shall be capable of being controlled manually by a train operator or automatically by the CBTC system (supervised by the train operator, if present), as specified by the authority having jurisdiction. When operating automatically, some functions (such as door operation and train departure initiation) may continue to be the responsibility of the train operator and/or conductor(s), if present.

4.5.1.2 Non-CBTC-equipped trains

Trains not equipped with train-borne CBTC equipment and/or trains with inoperative train-borne CBTC equipment that are operating in CBTC territory shall operate under the protection of an auxiliary wayside system and/or operating procedures, as specified by the authority having jurisdiction.

4.5.2 Failure mode train operations in CBTC territory

For light rail, heavy rail, and commuter rail applications operating with crews, it is an operational requirement to continue to move trains safely in the event of CBTC equipment and/or data communication failures,

possibly at reduced operating speeds and/or increased operating headways when compared to normal train operations. As a consequence, a CBTC system shall be designed to support degraded modes of operation in the event of failure and to continue to provide ATP with minimum reliance on adherence to operating procedures. This shall be achieved through functional elements of the CBTC system itself, an auxiliary wayside system (if specified by the authority having jurisdiction), or a combination of both systems.

For fully automated people mover applications operating without crews, the extent to which the CBTC system shall be designed to support degraded modes of operation in the event of failure shall be as defined by the authority having jurisdiction, and may include an ability to remotely reset train-borne equipment and the ability to support automatic push/pull train recovery, as well as the ability to support manual train operations and alternative routing strategies.

For all applications, a fall-back plan, based on failure analysis and operating procedures, shall identify train operating modes that will take advantage of the degraded modes of operation and recovery capabilities of the CBTC system. The goal of the plan shall be to eliminate hazards to passengers and staff in accordance with 5.3, while continuing to provide passenger service.

Specifically, failure mode train operations in CBTC territory shall address those CBTC system failures affecting the following:

a) All trains operating within a particular area of control

b) A particular train operating within any area of control

4.5.2.1 CBTC system failures affecting all trains operating within a particular area of control

In the event of a CBTC system failure that affects all CBTC-equipped trains operating within a particular area of control within CBTC territory (e.g., wayside CBTC equipment or wayside-to-train data communications failure), trains shall have the capability to provide continued safe operations under the control of a train operator, and

a) With the protection of an auxiliary wayside system (if specified by the authority having jurisdiction); or

b) Through strict adherence to operating procedures; or

c) A combination of both items a) and b).

When operating in this failure mode, ATP functions that reside within individual train-borne CBTC equipment shall continue to function to the extent safety can be assured.

4.5.2.2 CBTC system failures affecting a particular train operating within any area of control

In the event of a CBTC system failure affecting a particular CBTC-equipped train operating within any area of control within CBTC territory (e.g., train-borne CBTC equipment failure), that train shall be capable of continued safe operations under the control of a train operator, and

a) With the protection of an auxiliary wayside system (if specified by the authority having jurisdiction); or

b) With the train speed limited by the propulsion system; or

c) Through strict adherence to operating procedures; or

d) A combination of any or all of items a), b), and c).

When operating in this failure mode, ATP functions that reside within wayside CBTC equipment and within other train-borne CBTC equipment shall continue to function to the extent safety can be assured.

4.5.3 Normal train operating modes in non-CBTC territory

For the purposes of this standard, non-CBTC territory is defined as any territory that is not equipped with wayside CBTC equipment fully compatible with the train-borne CBTC equipment.

CBTC equipment installed on trains operating in non-CBTC territory shall include the necessary capabilities to support transitions into CBTC territory. In addition, if specified by the authority having jurisdiction, train-borne CBTC equipment may also perform other ATP functions while operating in non-CBTC territory, such as limiting train speed and/or providing zero speed detection.

If specified by the authority having jurisdiction, train-borne CBTC equipment operating in non-CBTC territory may also interface with wayside equipment that is not fully compatible with the train-borne CBTC equipment. In no case, however, shall the train-borne CBTC equipment provide an indication of standard CBTC operation when operating in non-CBTC territory, unless the applicable authority or authorities having jurisdiction over the train-borne and wayside equipment have ensured that standard CBTC operation is supported by the integrated train-borne and wayside systems.

4.5.4 Failure mode train operations in non-CBTC territory

Except where specified to perform certain ATP functions while operating in non-CBTC territory, failure of the train-borne CBTC equipment shall have minimal impact on train operation. The failure shall be indicated to the train operator, if present.

4.6 Entering/exiting CBTC territory

4.6.1 Entering into CBTC territory

A CBTC system shall have precise knowledge of the limits of CBTC territory and shall include the capability to perform verification checks of the train-borne CBTC equipment prior to entering CBTC territory. The checks shall be performed sufficiently in advance of entry into CBTC territory to verify the proper operation of the train-borne CBTC equipment (including any wayside CBTC equipment dependencies).

If the verification check is passed, an indication to this effect shall be provided. Under normal circumstances and subject to ATP constraints, it shall not be necessary for a train to come to a stop when entering CBTC territory unless required for other operational reasons.

In the event that the verification check fails, an indication of the CBTC system failure shall be provided, and train operation may revert to the auxiliary wayside signal system if available or to operating rules if no auxiliary wayside signal system is provided.

The results of the verification checks shall be displayed on the ATS user interface. For trains operating with crews, the results of the verification checks shall also be indicated to the train operator.

4.6.2 Exiting from CBTC territory

For trains operating with crews, prior to exiting CBTC territory, a CBTC system may provide a visual indication to the train operator of time and/or distance until the train will be exiting the CBTC territory. When known by the CBTC system, the train operator may also receive an indication of the type of train control system into which the train will be traversing.

NOTE—Indications to the train operator may not be required if the transition between CBTC territory and non-CBTC territory is operationally transparent to the train operator.

Under normal circumstances and subject to ATP constraints, it shall not be necessary for a train to come to a stop when exiting CBTC territory unless required for other operational reasons.

4.7 Train operating speeds

A CBTC system shall be capable of meeting the performance and functional requirements of this standard, over the full range of possible train operating speeds specified by the authority having jurisdiction.

5. Performance requirements

5.1 CBTC factors contributing to achievable headways

The required design and operating headways (i.e., the minimum and scheduled headways) for both normal and reverse directions shall be specified by the authority having jurisdiction. Headway may be specified as uninterfered and/or interfered.

In all cases, the design headway shall be constrained by the safe train separation requirements and the safe braking model of 6.1.2.1.

In the case of an uninterfered headway, a train speed profile shall not be affected by a preceding train. All trains shall, therefore, perform at the maximum allowed speed, depending on the civil speed limits and the acceleration and braking capabilities of the trains themselves. Operation at uninterfered headways facilitates a minimum end-to-end trip time for a given set of station dwell times.

Headways may be reduced (at the expense of increased trip times) with an interfered headway where a train speed profile is affected by a preceding train such that a following train decelerates on the approach to a station and enters the station area at a reduced speed. Interfered headway may also be specified to support multiple berthings at a station platform.

The design headway for a particular line and a particular set of vehicles involves many factors that are outside the control of the CBTC system (e.g., track alignment, gradients, civil speed limits, train acceleration and braking rates, station dwell times, terminal track configurations, driver reaction times). These factors shall be specified by the authority having jurisdiction. This standard addresses only those CBTC factors contributing to achievable headways, of which the most significant are the following:

a) Location (both accuracy of measured end-of-train locations and resolution of movement authority limits for a given train), including the frequency at which location reports and movement authorities are updated.
b) Speed, including both accuracy of speed measurement and resolution of speed limits established for a given train at a given location.
c) Communications delays, including nominal and worst-case transmission times of command/status messages between wayside and train, and vice versa. (Command/status messages include, for example, messages related to movement authority updates and/or location report updates.)
d) CBTC equipment reaction times, including maximum error accumulation, for both wayside and train-borne equipment, and for various operating modes, as applicable. (CBTC equipment reaction times include, for example, the time required to establish new movement authority limits following location report updates, the time to establish new movement authority limits through an interlocking, and the time to determine a new ATP profile following movement authority update.)
e) CBTC system performance limitations (e.g., the maximum number of trains that can be processed by the CBTC system, within a given area of control).
f) CBTC automatic speed regulation algorithm.

Typical values for the CBTC parameters in items a) through e) are given in Annex C.

5.2 CBTC factors contributing to achievable trip times

Trip time requirements shall be specified by the authority having jurisdiction, consistent with train performance and track alignment characteristics.

The minimum end-to-end trip times for a defined set of station dwell times will result from uninterfered headway speed profiles. The CBTC factors contributing to achievable headways, as identified in 5.1, will also be factors contributing to the minimum achievable trip times.

5.3 System safety requirements

5.3.1 CBTC System Safety Program requirements

A System Safety Program shall be instituted during the CBTC system planning/design phase and shall continue throughout the system life cycle. The CBTC System Safety Program shall emphasize the prevention of accidents by identifying and resolving hazards in a systematic manner. A CBTC System Safety Program Plan (SSPP) shall be developed for each CBTC application. The CBTC SSPP shall be prepared in accordance with the requirements of E.1 of Annex E or the requirements of the American Public Transit Association's Manual [B1] or equivalent requirements, as approved by the authority having jurisdiction.

Implementation of the CBTC SSPP shall specifically recognize configuration management issues, given the importance of software and hardware configuration control in maintaining system safety.

5.3.2 CBTC hazard identification and risk assessment process

Hazard analyses shall be employed during the design of a CBTC system to assist in the identification and evaluation of potential hazards to assess their likelihood and severity and to document their resolution. As a minimum, a preliminary hazard analysis (PHA) shall be conducted for each new CBTC system project. Other detailed analyses, including system/subsystem hazard analyses, failure modes, effects and criticality analyses, fault tree analyses, and operational and support hazard analyses, shall also be conducted if mandated by the CBTC SSPP. These analyses shall be conducted in accordance with E.2, E.3, E.4, and E.5 of Annex E or equivalent requirements, as approved by the authority having jurisdiction.

All hazards identified through the CBTC System Safety Program shall be assessed in terms of the severity or consequence of the hazard and the probability of occurrence. This shall be accomplished in general accordance with the criteria outlined in E.6 of Annex E or the equivalent, as approved by the authority having jurisdiction. Risk assessment estimates shall be used as the basis in the decision-making process to determine whether individual system or subsystem hazards shall be eliminated, mitigated, or accepted. This process shall include full documentation of the hazard resolution activities.

Hazards shall be resolved through a design process that emphasizes the elimination of the hazard. The effectiveness of the hazard resolution strategies and countermeasures shall be monitored to determine that no new hazards are introduced. In addition, whenever substantive changes are made to the system, analyses shall be conducted to identify and resolve any new hazards.

As a minimum, a CBTC system shall address the following critical/catastrophic system hazards through the implementation of the ATP functions defined in 6.1:

a) Train-to-train collisions (rear-end, sideswipe, head-on); hazard to be addressed through train separation assurance (see 6.1.2), rollback protection (see 6.1.4), parted consist protection (see 6.1.6), route interlocking protection (see 6.1.11), and traffic direction reversal interlocks (see 6.1.12)
b) Train-to-structure collisions; hazard to be addressed through end-of-track protection (see 6.1.5) and restricted route protection (see 6.1.16)
c) Train derailments; hazard to be addressed through overspeed protection (see 6.1.3), route interlocking protection (see 6.1.11), and (where specified by the authority having jurisdiction) broken rail detection (see 6.1.14)
d) Collisions between trains and highway vehicles (where highway crossing at grade exists within the limits of CBTC territory); hazard to be addressed through grade-crossing warning devices that may include interfaces to the CBTC system (see 6.1.15)
e) Hazards to work crews and work trains; hazards to be addressed through CBTC work zone protection functions (see 6.1.13)
f) Hazards to passengers associated with train movement with train doors open; hazards to be addressed through interface between the CBTC system and the train door system (where required by the authority having jurisdiction) to provide door opening control protection interlocks (see 6.1.8), zero speed detection (see 6.1.7), and departure interlocks (see 6.1.9)
g) Hazards associated with collisions with objects on the track; hazards to be addressed through interfaces between the CBTC system and intrusion detection devices (where specified by the authority having jurisdiction) (see 6.1.16)

5.3.3 CBTC vital functions

To eliminate or control to a level acceptable to the authority having jurisdiction those hazards judged to be unacceptable or undesirable through the risk assessment process of 5.3.2, a CBTC system shall include, as a minimum, the vital functions identified in 6.1.

All vital functions of a CBTC system shall be designed and implemented in accordance with fail-safe principles. Documentation of the means used, and proof that fail-safe principles have been met and the mean time between hazardous event (MTBHE) requirements of 5.3.4 have been satisfied, shall be required for every CBTC system.

Verification that the processor-based portions of a CBTC system meet these minimum system safety requirements shall be completed in accordance with IEEE Std 1483-2000.[6]

5.3.4 Quantitative CBTC safety performance requirements

For any CBTC system application, the CBTC wayside and train-borne equipment located within any 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 shall have a total calculated aggregate MTBHE (total of all critical and catastrophic hazards) of at least 10^9 operating hours. This includes the maximum number of other trains that can be located in this contiguous portion of a one-way route under the specified peak operating headway. System safety documentation shall support these calculations and substantiate the methodology used to arrive at the result. For the purposes of MTBHE calculations, a hazardous event shall include, as a minimum, the occurrence of any of the specific hazards identified in 5.3.2.

NOTE—If the end-to-end trip time for a given route is greater than 1 h, the MTBHE requirement for that route would be adjusted proportionately. As an illustrative example, if the specified end-to-end trip time (per 5.2) for a given one-way route is 2 h, and if the route includes 4 sets of wayside CBTC equipment, and if a maximum of 10 trains can be operating on the route at a given time (when operating at the specified peak headway, per 5.1), then the MTBHE of the combined 4 sets of wayside CBTC equipment and 10 sets of train-borne CBTC equipment on that route would be at least 0.5×10^9 operating hours.

[6]Information on references can be found in Clause 2.

5.3.5 Basic safety design principles

5.3.5.1 Normal transit system operations with no CBTC hardware failures

A CBTC system shall respond safely and correctly perform all ATP functions within the normal range of inputs and other operating and environmental conditions.

All conditions necessary for the existence of any permissive state or action shall be verified to be present before the permissive state or action is initiated by a CBTC system. The requisite conditions shall be verified to be continuously present for the permissive state or action to be maintained.

System safety shall not depend on the correctness of actions taken or procedures used by operating personnel.

Procedures shall not be considered a substitute for safety functions that are to be vested in specific CBTC components or equipment.

5.3.5.2 Abnormal transit system operations with no CBTC hardware failures

A CBTC system shall respond safely under conditions of abnormal system loading, abnormal/improper inputs, and other abnormal external influences such as electrical, mechanical, and environmental factors.

5.3.5.3 Response to CBTC hardware failures

A CBTC system shall respond safely under conditions of credible hardware failure.

NOTE—The AREMA Communications & Signals Manual, Part 17.3.3 [B2], provides examples of credible hardware failures.

Failure to perform a logical operation or absence of a logical input, output, or decision shall not cause an unsafe condition, i.e., system safety shall not depend upon the occurrence of an action or logical decision.

Hazard analyses shall consider all credible CBTC hardware failure modes. Justification shall be provided for conceivable failure modes that are not considered credible. The effect of each credible CBTC failure mode shall be classified as either self-revealing or non-self-revealing, as follows:

— No credible single point CBTC hardware failure, whether self-revealing or non-self-revealing, shall cause an unsafe condition.

— No credible CBTC hardware failure in combination with one or more non-self-revealing failure shall cause an unsafe condition. In the instance of a non-self-revealing failure, a subsequent failure shall not be considered independent.

— The probability of a critical or catastrophic hazard arising as a result of combinations of simultaneous independent self-revealing failures shall be considered in the calculated CBTC MTBHE.

5.3.5.4 Recovery from CBTC hardware failures

A combination of functional elements of the CBTC system itself, an auxiliary wayside system (if specified by the authority having jurisdiction), and/or operating procedures shall provide for the safety of train movement under failure conditions, including failure recovery.

5.4 System assurance requirements

5.4.1 General

The ability of a CBTC system to accomplish the functional requirements of this standard, under normal conditions and under conditions of equipment failure, is of paramount importance to the authority having jurisdiction. This subclause establishes qualitative availability, reliability, and maintainability criteria for CBTC systems and equipment in order to meet or exceed the on-time performance and fleet availability objectives of the authority having jurisdiction, and thereby minimize delays experienced by passengers. In addressing CBTC equipment failures, a distinction shall be made between the following failure types:

a) *Type 1:* Those failures, or combination of failures, that impact on-time performance of the transit system.

b) *Type 2:* Those failures, or combination of failures, that do not impact on-time performance of the transit system, but do result in some other loss of specified CBTC functionality.

c) *Type 3:* Those failures that do not impact on-time performance of the transit system or result in a loss of any specified CBTC functionality (e.g., because of equipment redundancy).

The CBTC system availability requirement (see 5.4.2) shall include consideration of all Type 1 failures, as well as the mean time to restore service (MTTRS) for Type 1 failures.

The CBTC system mean time between functional failure (MTBFF) requirement (see 5.4.3) shall include consideration of all Type 1 and Type 2 failures.

The CBTC system mean time between failure (MTBF) requirement (see 5.4.3) shall include consideration of all Type 1, Type 2, and Type 3 failures.

While system availability, system MTBFF, and system MTBF predictions traditionally consider only hardware failures, measurements of achieved system availability, system MTBFF, and system MTBF shall also consider software errors (i.e., software fails to perform intended function) as well as hardware failures.

The following general recommended practices apply:

1) Components and materials should be selected and appropriate standards of quality control and test procedures should be employed to ensure the lowest practical hardware failure rates for individual items of CBTC equipment (i.e., maximize the hardware portion of the system MTBF).

2) Unless non-redundant equipment is sufficiently reliable to satisfy the overall system availability requirements, appropriate levels of equipment redundancy should be employed such that the failure of a single component, processor, or device will not render the CBTC system unavailable or an operationally critical function nonoperative (i.e., maximize the system MTBFF).

3) A CBTC system should incorporate degraded modes of operation to minimize the operational impacts of equipment failures and to permit train movements to continue safely (i.e., maximize system availability).

4) CBTC system downtime or unavailability of an operationally critical function should be minimized through the use of local and remote diagnostic capabilities and appropriate operating and maintenance procedures [i.e., minimize mean time to repair (MTTR)].

5.4.2 System availability requirements

Quantitative CBTC system availability requirements shall be established by the authority having jurisdiction with appropriate consideration of the impacts of CBTC system and subsystem failures on the operation of the transit system. Typical methods for defining CBTC system availability are provided in Annex F.

As specified by the authority having jurisdiction, system availability analysis/modeling shall be used to predict the system availability for a given CBTC system configuration, based on equipment reliability/ maintainability calculations, equipment redundancy provisions, and other defined assumptions.

As specified by the authority having jurisdiction, system availability demonstration tests shall be performed to determine actual CBTC system availability over a defined period, to a given confidence level.

5.4.3 Equipment reliability requirements

Quantitative CBTC system and subsystem MTBF and MTBFF requirements shall be established by the authority having jurisdiction, consistent with the CBTC system availability requirement of 5.4.2.

5.4.3.1 Design life

CBTC equipment shall have a design life of 30 y.

NOTE—The ability of a CBTC system to remain in operation to the end of its design life will be driven largely by long-term availability of spare parts. Specific requirements with respect to spare part availability shall be defined by the authority having jurisdiction and do not form part of this standard.

5.4.4 Equipment maintainability requirements

A CBTC system shall be designed to minimize required maintenance (both preventive and corrective) by maximizing the system MTBF and by including features that provide for ease of maintenance by maintenance personnel.

The mean time to repair/replace a failed piece of in-service CBTC equipment (i.e., first-level repair) shall include on-site diagnostics, the replacement of failed components, and the testing of the repaired units, subsystem, or system, but shall exclude travel time to the site. A separate MTTR requirement may be defined for second-level repair (i.e., shop repair of a failed line replaceable unit).

The first-level MTTR shall be no greater than 30 min. The second level MTTR, if specified, shall be no greater than 2 h.

Achievable repair times will be driven by equipment diagnostic provisions and available test equipment, as well as the quality of the maintenance manuals and training. A CBTC system shall, therefore, include maintenance and diagnostic capabilities to detect and react to CBTC equipment failures. This shall include remote diagnostics capabilities as well as local built-in test equipment and other fault displays for trouble-shooting, and the timely identification of failed components and functions.

Data logging capabilities shall also be provided in wayside and train-borne CBTC equipment. The logged data shall be capable of being analyzed to be able to recreate the sequence of events leading to an incident. This will allow maintenance personnel to identify the cause of any failure and/or mis-operation of CBTC equipment that cannot be identified by the in-built diagnostics of the equipment. The scope of logged CBTC events shall be established by the authority having jurisdiction.

A CBTC system design shall include capabilities to permit periodic verification of ATP hardware, software, and data, including verification of correct response to interference on the train-to-wayside data link. To the extent specified by the authority having jurisdiction, a CBTC system shall also include capabilities to facilitate modifications (by the user) to CBTC system parameters, track databases, and applications software. The supplier of the CBTC system shall identify to the authority having jurisdiction those specific changes to CBTC system parameters, track databases, and applications software that will have no impact on system safety.

WARNING

Changes made to CBTC system parameters, track databases, and application software, other than those identified by the supplier as not impacting safety, can affect safe system operation. Prior to implementing any such changes, applicable hazard analyses of 5.3.2 shall be reassessed to verify that the modified system will still meet all requirements of this standard including, but not limited to, 5.3.3, 5.3.4, and 5.3.5. Changes shall be implemented in accordance with the CBTC SSPP of 5.3.1.

5.5 Environmental requirements

Train-borne CBTC equipment shall comply with the requirements of IEEE Std 1478-2001.

Wayside CBTC equipment shall comply with the requirements of IEEE P1582/D1.0.

6. Functional requirements

A CBTC system shall include the capability for providing ATP, ATO, and ATS functions. ATP functions shall provide fail-safe protection against collisions, excessive speed, and other hazardous conditions. ATP functions shall have precedence over both the ATO and ATS functions. ATO functions shall control basic operations that would otherwise be performed by a train operator and shall do so within the protection limits imposed by ATP. ATS functions shall provide system status information and the means to monitor and override the automatic control for various functions of the system.

The CBTC train-to-wayside communications interface shall be sufficient to support all required ATP, ATO, and ATS functions. The data link shall provide continuous geographic coverage within CBTC territory and shall support train operations in tunnels, tubes, and cuts, on elevated structures, and at grade. The data link shall support bidirectional data transfer and shall exhibit sufficiently low latency to support the defined performance requirements. The data link shall include a protocol structure to support safe, timely, and secure delivery of train control messages.

6.1 ATP functions

All ATP functions shall be vital functions and shall be designed and implemented in accordance with 5.3.

A CBTC system shall be capable of providing bidirectional ATP.

6.1.1 Train location/train speed determination

6.1.1.1 CBTC train location/train speed determination

CBTC train location/train speed determination shall be a required ATP function for any CBTC system configuration.

A CBTC system shall establish the location, speed, and travel direction of each CBTC-equipped train operating in CBTC territory.

CBTC train location determination shall safely and accurately establish the location of both the front and rear of the train. The CBTC train location determination function shall provide sufficient train location resolution and accuracy to support the performance and safety requirements of this standard. Train location resolution and accuracy parameters for typical CBTC systems are included in Annex C.

The CBTC train location determination function shall be self-initializing and shall automatically detect and establish the location of each CBTC-equipped train as it enters CBTC territory and on recovery from CBTC equipment failures, without requiring manual input of train location or train length data.

The CBTC train speed determination function shall provide sufficient speed measurement resolution and accuracy to support the performance and safety requirements of this standard. Speed measurement resolution and accuracy parameters for typical CBTC systems are included in Annex C.

A CBTC system shall compensate for the effects of measurement inaccuracies on train location and speed determination. Specifically, if the CBTC train location/speed determination function is dependent upon wheel rotation, the CBTC system shall correct for position errors induced by the slipping or sliding of wheels and shall correct for position errors caused by variation in wheel size due to wear, trueing, or replacement.

6.1.1.2 Secondary train location determination

If specified by the authority having jurisdiction, an auxiliary wayside system may provide secondary train location determination to establish if a section of track is occupied by one or more trains, including trains not equipped with train-borne CBTC equipment and/or trains with inoperative train-borne CBTC equipment. It will not be necessary to determine the location of non-CBTC-equipped trains, or trains with inoperative train-borne CBTC equipment, to the same accuracy as CBTC-equipped trains.

6.1.2 Safe train separation

Safe train separation shall be a required ATP function for any CBTC system configuration.

Safe train separation shall be provided between all trains operating in CBTC territory, whether or not the trains are CBTC equipped.

A CBTC system shall provide safe train separation between CBTC-equipped trains. Safe train separation shall be based upon the principle of an instantaneous (brick wall) stop of the preceding train.

For mixed-mode operation (see 4.5), safe train separation shall be provided through an auxiliary wayside system and/or through strict adherence to operating procedures, as specified by the authority having jurisdiction.

If secondary train location determination is provided through an auxiliary wayside system (see 6.1.1.2), then for a CBTC-equipped train following a non-CBTC-equipped train or a train with inoperative train-borne CBTC equipment, a CBTC system shall limit the movement authority of the following train to the boundary of the section of track occupied by the non-CBTC-equipped or failed train. If specified by the authority having jurisdiction, the CBTC system may further limit the movement authority to the route entry point of a route occupied by the non-CBTC-equipped train or failed train.

The CBTC safe train separation function shall consist of the following:

a) The calculation of the ATP profile (i.e., the profile of safe speed as a function of train location), derived from fixed ATP data (e.g., permanent speed limits) and variable ATP data (e.g., temporary speed limits and movement authority limit)
b) The supervision and enforcement of the ATP profile calculated by the CBTC system

The ATP profile shall be governed by a safe braking model (see 6.1.2.1) and shall ensure that under no circumstances (including failures) will the movement authority limit be exceeded by a CBTC-equipped train.

The movement authority limit shall be the most restrictive of the following:

— The rear of a CBTC-equipped train ahead (as determined by the CBTC train location function in 6.1.1.1), with allowance for any location uncertainty
— The boundary of a section of track occupied by a non-CBTC-equipped train or a train with inoperative train-borne CBTC equipment (as determined by an auxiliary wayside system, if provided, per 6.1.1.2)
— The end-of-track (see 6.1.5)
— The entrance to an interlocking, when the route is not verified as aligned and locked (see 6.1.11)
— The boundary of a section of track with an opposing traffic direction established (see 6.1.12)
— The boundary of a blocked track (see 6.1.13)
— If specified by the authority having jurisdiction, the entrance to a highway grade crossing where warning devices are not confirmed to be operating (see 6.1.15)
— The entrance to a route that is detected to be unsafe for train movement (see 6.1.16)

If specified by the authority having jurisdiction, the CBTC safe train separation function shall support automatic close-up of trains and automatic coupling and uncoupling of trains in designated areas.

If specified by the authority having jurisdiction, facilities may be provided to bypass the CBTC safe train separation function to allow a train, under the control of a train operator, to travel beyond its movement authority limit (e.g., at a restricted speed), for failure recovery purposes.

If specified by the authority having jurisdiction, facilities may be provided to pull back (i.e., make more restrictive) a movement authority limit previously granted to a train. If the train were approaching or braking toward the original movement authority limit, the train may be in violation of the new ATP profile. Under such circumstances, a CBTC system shall initiate an immediate brake application. The brake application may be an immediate emergency brake application or a supervised service brake application, as specified by the authority having jurisdiction (see 6.1.3).

6.1.2.1 Safe braking model

A safe braking model shall be developed for each CBTC application.

The safe braking model shall, as a minimum, include consideration of the following:

a) Location uncertainty of lead train (including rollback tolerance)
b) Location uncertainty of following train
c) Train length
d) Train configuration (see 4.4)
e) Allowable overspeed permitted by the CBTC system
f) Maximum CBTC speed measurement error
g) CBTC system reaction times and latencies
h) Maximum train acceleration rate possible at the time an overspeed condition is detected by the CBTC system
i) Worst-case reaction times to disable the propulsion system and apply the emergency brakes following detection of an overspeed condition by the CBTC system
j) Guaranteed emergency brake rate (GEBR)
k) Grade

The GEBR shall be the minimum emergency brake rate achieved by a train on level tangent track under the range of environmental conditions and worst-case credible latent brake equipment failure modes, which can be anticipated to exist for that train in the specific application. The GEBR shall be specified by the authority

having jurisdiction and shall include consideration of maximum passenger load (plus snow and ice load if applicable), minimum anticipated adhesion levels, and maximum design tailwind.

A typical safe braking model is provided in Annex D.

A CBTC system shall have the capability to support multiple safe braking models to accommodate different train acceleration/braking rates for different classes and configurations of trains operating simultaneously within CBTC territory and to accommodate automatic close-up and automatic coupling/uncoupling capabilities, as specified by the authority having jurisdiction. A CBTC system shall incorporate appropriate protection to ensure that the correct safe braking model is applied for a given train at a given location.

6.1.3 Overspeed protection and brake assurance

Overspeed protection shall be a required ATP function for any CBTC system configuration.

In establishing, supervising, and enforcing the ATP profile, as governed by the safe braking model of 6.1.2.1, a CBTC system shall ensure that under no circumstances, including failures, will the train's actual speed exceed its safe speed. The safe speed shall be derived by considering the most restrictive of the following:

a) The permanent speed limits on sections of track within the ATP profile

b) Any temporary speed restrictions on sections of track within the ATP profile

c) Any permanent speed restriction applicable to the particular class or configuration of train

d) Any speed restrictions enforced on the train because of train-borne failure conditions

e) The maximum speed that would allow the train to stop safely prior to the limit of the train's movement authority or to slow down sufficiently to meet appropriate permanent or temporary speed restrictions upon entering that section of track

Speed limits and restrictions shall apply when any portion of the train is within the speed limit area.

Speed limit/speed restriction resolution parameters for typical CBTC systems are included in Annex C.

Enforcement of the calculated ATP profile shall be achieved by comparing the CBTC-determined train speed with the ATP profile speed at the CBTC-determined train location. If the ATP profile speed at that location is exceeded, the CBTC system shall initiate an immediate brake application.

The brake application may be an immediate emergency brake application or a supervised service brake application, as specified by the authority having jurisdiction. In the latter case, a CBTC system shall monitor the achieved brake rate to ensure an acceptable brake rate is achieved within a predetermined time frame; if not, it shall immediately apply the emergency brakes. The safe braking model shall include appropriate allowances for reaction times associated with this brake assurance function.

6.1.4 Rollback protection

Rollback protection shall be a required ATP function for any CBTC system configuration.

A CBTC system shall monitor actual train travel direction and shall compare measured travel direction with the CBTC established/commanded direction of traffic. Train motion against traffic for more than a specified rollback tolerance shall result in the CBTC system initiating an emergency brake application. Rollback detection criteria for typical CBTC systems are included in Annex C.

6.1.5 End-of-track protection

End-of-track protection shall be a required ATP function for any CBTC system configuration that permits the operation of trains up to, or in close proximity to, an end-of-track terminus.

End-of-track protection shall be incorporated into, or function in conjunction with, overspeed protection to prevent trains from over-traveling the end-of-track or, if buffers are specified, to prevent trains from exceeding the design limits for impact with an end-of-track buffer. End-of-track protection design shall be based on the safe braking model of 6.1.2.1.

6.1.6 Parted consist protection and coupling and uncoupling of trains

Where separate vehicles can be coupled together in a consist of two or more vehicles or units to form a train, a CBTC system shall have the capability of detecting and protecting parted trains. Parted consist protection shall be required regardless of whether the individual vehicles or units are considered to be permanently coupled or whether they are routinely uncoupled for maintenance or operational purposes.

A CBTC system shall also support operating requirements for coupling and uncoupling of trains, including automatic update of the consist length within the CBTC system.

If specified by the authority having jurisdiction, a CBTC system may assume a fixed, worst-case, maximum train length for a given class of trains operating in CBTC territory, with a reliance on operating procedures to ensure this maximum train length is not exceeded.

6.1.7 Zero speed detection

Zero speed detection shall be a required ATP function for any CBTC system configuration and shall be in accordance with the requirements of 5.10 of IEEE Std 1475-1999.

Zero speed detection criteria for typical CBTC systems and applications are included in Annex C.

6.1.8 Door opening control protection interlocks

If trains are operated with crews, door open control protection interlocks may be a required ATP function, at the option of the authority having jurisdiction. For operation of trains without crews, door open control protection interlocks shall be mandatory. These interlocks, if provided, shall ensure that the following conditions are satisfied prior to enabling the opening of the train doors (and platform doors, if fitted):

a) The train is “properly aligned” at a designated stopping point, where the designated stopping point and required tolerances shall be as specified by the authority having jurisdiction.

b) There is a platform (or other location specified by the authority having jurisdiction) on the side of the train for which the door opening is allowed.

c) Zero speed is detected, in accordance with 6.1.7.

d) The train is constrained against motion.

Selective door open enable shall be possible for those applications where the train length exceeds the platform length.

If specified by the authority having jurisdiction, facilities may be provided for a local manual bypass of the preceding door open control protection interlocks, for failure recovery purposes.

6.1.9 Departure interlocks

If trains are operated with crews, departure interlocks may be a required ATP function, at the option of the authority having jurisdiction. For operation of trains without crews, departure interlocks shall be mandatory. These interlocks, if provided, shall prevent a stationary train from moving (e.g., by disabling the propulsion system) unless all train doors (and platform edge doors, if fitted) are properly closed and locked, in accordance with the requirements of 5.14 of IEEE Std 1475-1999.

If specified by the authority having jurisdiction, facilities may be provided for a local manual bypass of the preceding departure interlocks, for failure recovery purposes.

6.1.10 Emergency braking

The train's emergency brake system shall be capable of bringing the train to a stop within the assured stopping distance determined by the safe braking model of 6.1.2.1. Specific criteria for resetting the emergency brakes to allow normal operation to resume shall be specified by the authority having jurisdiction. If conditions (as determined by ATP) are not correct for train movement, the emergency braking shall remain applied regardless of any reset signals or actions, except that facilities may be provided for a local manual bypass of the ATP functions for that train to permit manual train operation for failure recovery purposes. Use of such facilities shall require strict adherence to operating procedures to ensure the safety of train movements. If correct ATP conditions exist after the emergency brakes have been reset, the train shall be permitted to move or continue to move; however, if the actual train speed again exceeds the ATP profile speed or a subsequent malfunction occurs, emergency braking shall be applied as before.

6.1.11 Route interlocking

A CBTC system shall provide route interlocking functions equivalent to conventional interlocking practice to prevent train collisions and derailments. These functions shall include locking of the route in advance of the train entering the interlocking (time or approach locking) and once the train is in the interlocking (route locking). The switches shall also be locked when the track section containing the switch is occupied by a train (detector locking). Locking functions shall also apply to moveable bridges and similar right-of-way apparatus. Sectional release (of routes behind a train) may be provided where specified by the authority having jurisdiction.

NOTE—The AREMA Communications & Signals Manual, Sections 2 and 16 [B2], provides examples of recommended practices for use in interlocking design.

A movement authority shall not be advanced into an interlocking until the appropriate route is set and locked. Once a movement authority has been advanced through an interlocking, the affected route shall not be released and conflicting routes cleared unless either the train has traveled through and is verified clear of the interlocking or the movement authority is pulled back short of the interlocking and is in effect.

Where an auxiliary wayside system is specified by the authority having jurisdiction, interlocking functions may be provided by separate interlocking equipment, which is based on train position established by a secondary train detection subsystem. In this case, a CBTC system shall interface to and may modify the conventional interlocking functions based on train position established by the CBTC train location determination function, to safely enable the enhanced performance capabilities of a CBTC system to be realized.

6.1.11.1 CBTC interfaces to a separate interlocking

Where an auxiliary wayside system or separate interlocking is specified, a CBTC system shall interface to interlockings as follows:

a) Time or approach locking shall apply, except in the event of a route being canceled for an approaching CBTC train (i.e., the movement authority is pulled back short of the interlocking and is in effect). In this case, if the train is greater than a safe braking distance from the entrance to the interlocking (as determined by the safe braking model of 6.1.2.1) or the train stops prior to entering the interlocking, the route shall be released without running further time.

b) Traffic locking may be overridden so that CBTC-equipped trains may move in opposing directions within their respective movement authorities on the same track at the same time.

c) Wayside signals and their aspects may be provided as specified by the authority having jurisdiction. A CBTC system may override the conventional aspects to cause the signal(s) to display CBTC aspect(s) only to CBTC-equipped trains.

6.1.11.2 Responses to CBTC train location failures

In the event of a failure of the CBTC train location determination function, route locking shall remain in effect until the train is proven to be clear of the interlocking by the CBTC system (i.e., the train is subsequently determined to be clear of the interlocking limits), or through operating procedures, or a combination of both approaches.

In the event of a failure of the CBTC train location determination function in an interlocking where train location is also capable of being detected by means of a secondary system, CBTC system overrides of the interlocking functions may be released, provided route and other locking functions are maintained by the auxiliary wayside system so as to prevent the movement of a switch in front of and under the train until the train is proven to be clear of the interlocking.

6.1.11.3 Response to loss of switch indication

In the event of a loss of switch indication once a movement authority has been issued through an interlocking, a CBTC system shall pull back the movement authority to the entrance of the interlocking. If a train is already within a safe braking distance of the switch, the CBTC system shall initiate an immediate brake application (see 6.1.2).

6.1.12 Traffic direction reversal interlocks

Traffic direction reversal interlocks shall be a required ATP function for any CBTC system application requiring bidirectional operations, in order to support reversal of train direction at terminal stations and to support intermediate turn backs and shuttle modes of operation, for example.

It shall not be possible to extend the movement authority for a train into a section of track where an opposing traffic direction has already been established.

A reversal of traffic direction within a section of track shall not be possible unless

a) All trains within that section of track are at zero speed and constrained against motion in the original traffic direction, and

b) The movement authorities for all trains outside of that section of track do not extend into the section and are constrained from being extended into the section in the original traffic direction.

6.1.13 Work zone protection

A CBTC system shall not grant movement authorities to trains to operate into out-of-service (blocked) tracks or through switches blocked in other than the required position and shall enforce restricted speeds on approach to and through defined work zones (see 6.3.7.4). A CBTC system may also include capabilities to preclude ATO mode of operation through a work zone.

6.1.14 Broken rail detection

Where specified by the authority having jurisdiction, a CBTC system may interface to an auxiliary wayside system for purposes of broken rail detection. A CBTC system's reaction to a detected broken rail shall be as specified by the authority having jurisdiction.

6.1.15 Highway grade-crossing warning

Where highway crossings at grade exist within the limits of CBTC territory and where specified by the authority having jurisdiction, a CBTC system may interface to grade-crossing warning devices to permit control of such devices based on CBTC location reports and to coordinate movement authorities through the crossing based on the status from such devices. Specific requirements shall be defined by the authority having jurisdiction and may include the following:

a) Constant (and consistent) warning times, independent of train speed or acceleration/deceleration
b) For trains making station stops prior to crossings, delayed activation of the warning devices until the train is ready to depart the station
c) When a train clears a crossing in multiple track areas, continued activation of the warning devices if a second train would have reactivated the devices within a predefined time interval
d) Advance warning for priority control of traffic lights or other highway signage, in accordance with IEEE Std 1570-2002 and/or the AREMA Communications & Signals Manual, Part 3.1.10 [B2].

6.1.16 Restricted route protections

Where specified by the authority having jurisdiction, a CBTC system shall include capabilities to prevent a train from entering a route that is unsafe for movement of that type of train due to mechanical, civil, electrical, or other predefined temporary or permanent conditions of the train or route, or through interfaces to intrusion detection devices, platform edge doors (where fitted), and/or other devices capable of detecting hazards that impact route integrity.

6.2 ATO functions

For operation of trains without crews, a CBTC system shall, as a minimum, be capable of providing all of the ATO functions as defined in this subclause, to automatically operate trains in accordance with prescribed operating criteria within the safety constraints imposed by ATP.

For operation of train with crews, the required ATO functions shall be as specified by the authority having jurisdiction.

The CBTC wayside-to-train and train-to-wayside data communications interface shall be sufficient to support all required ATO functions.

6.2.1 Automatic speed regulation

The starting, stopping, and speed regulation of the train as it travels along the track shall be automatically controlled by a CBTC system so that the speed, acceleration, deceleration, and jerk rates are within specified passenger comfort limits (as defined by the authority having jurisdiction) and the train speed is below the overspeed limits imposed by ATP.

Station stopping accuracy shall be as specified by the authority having jurisdiction.

A CBTC system shall support multiple ATO speeds, acceleration, and service brake rates in accordance with the train operator (if present) or ATS inputs.

6.2.2 Platform berthing control

A CBTC system shall be capable of implementing any of the following platform berthing control modes:

a) Where the platform length is approximately equal to the train length, a CBTC system shall allow a train to enter a station platform only if there is sufficient room to fully berth or if the preceding train has a movement authority that shall allow it to fully leave the platform area and it has begun to move out of the station (i.e., within ATP constraints, train movement shall be controlled to minimize the likelihood of the train coming to a stop when only partially within the station platform limits).

b) Where the platform length is longer than the train length, a CBTC system shall support multiple stopping positions within the platform area, as defined by the authority having jurisdiction.

c) Where the platform length supports multiple train berthings, a CBTC system shall allow a train to enter a platform while another train already occupies an alternative berth.

d) Where the platform length is shorter than the train length, a CBTC system shall support platform berthings consistent with the door opening control protection interlocks of 6.1.8.

6.2.3 Door control

A CBTC system shall be capable of automatically controlling train doors (and platform edge doors, where fitted) during passenger boarding and discharging.

As defined by the authority having jurisdiction, automatic door control may be limited to the following:

a) Automatic door opening only (with or without passenger door open requests)

b) Automatic door closing only

c) Neither automatic door opening nor closing

If automatic platform edge doors are provided, they shall be controlled as a set with the matching train doors such that the train and matching platform edge doors open and close together. It shall be possible to manually disable the operation of any door set (both the train and the matching platform edge door) without affecting the automatic operation of other door sets. The amount of time the train is to remain in the station with doors open may be established by ATS (6.3.5.1) and automatically controlled by ATO.

6.3 ATS functions

6.3.1 General

If specified by the authority having jurisdiction, a CBTC may interface to, or be integrated with, an ATS system. Under such circumstances, and to the extent specified by the authority having jurisdiction, CBTC-related ATS functions shall be implemented as defined in this subclause in order to benefit from the characteristics of a CBTC system as defined in 4.1, namely, the availability of the following:

— Train location information to a high precision, independent of track circuits

— Continuous wayside-to-train and train-to-wayside data communications link

— Train-borne and wayside data processing capabilities

The CBTC-related ATS functions defined in this subclause shall be fully integrated with other conventional ATS functions and other non-ATS functions, as may be specified by the authority having jurisdiction, to support overall service management for the transit system and provide for a single consistent user interface.

The CBTC data communications network, inclusive of the wayside-to-train and train-to-wayside data communications interface, shall be sufficient to support those CBTC-related ATS functions specified by the authority having jurisdiction.

6.3.2 ATS user interface

Each ATS user interface shall display all information and implement all control actions, as defined in 6.3, within acceptable latencies as specified by the authority having jurisdiction.

Mandatory display data and user information inputs shall be in accordance with IEEE Std 1474.2-2003.

The ATS user shall be able to override any automated CBTC-related ATS functions defined in 6.3.

Certain ATS functions (such as stopping a train en route and the application and removal of temporary speed restrictions, switch/track blocking, or work zones) can potentially introduce system hazards and the specific implementation of these functions shall be considered in the hazard analyses required by 5.3.2. ATS functions are not required to be implemented in a fail-safe manner; however, the hazard analyses shall take into account, as a minimum, the probability of

a) Safety-related commands not being executed when initiated by an ATS user,
b) The CBTC system prematurely removing safety-related commands initiated by an ATS user,
c) The CBTC system executing safety-related commands that were not initiated by an ATS user,
d) Incorrect information being displayed by the CBTC system to the ATS user.

The hazard analyses shall give due consideration of the specific transit application and whether the trains are operated with or without crews.

Control action confirmation shall be provided for any safety-related user interfaces/inputs and functions whose inadvertent implementation could have an adverse operational impact, as defined by the authority having jurisdiction.

6.3.3 CBTC train identification and train tracking

Each CBTC-equipped train operating within CBTC territory shall be assigned a train identification. This train identification shall indicate the type of train and other pertinent information about the train.

An ATS system shall have the capability to automatically track, maintain records of, and display on the ATS user interface the locations, identities, train schedule, and other pertinent data for all CBTC-equipped trains operating in the CBTC territory. The front and rear position of trains shall be tracked based on CBTC train location reports, and the train location shall be displayed on the ATS user interface. Variations in train length may be displayed either proportionally or as a standard length icon supplemented by textual train length data.

6.3.4 Train routing

An ATS system shall have the capability to permit CBTC-equipped trains operating in CBTC territory to be manually and automatically routed based on CBTC train location reports and in accordance with the train service data, predefined routing rules, and any ATS user-directed service strategy. Where applicable to the specific track configuration, automatic routing shall facilitate the proper merging and diverging of trains at junctions, turn back of trains, the movement of trains from/to storage areas, and the rerouting of trains in response to service disruptions and/or planned outages. Train routes shall be indicated on the ATS user interface and may also be indicated to the train operator and/or conductor, if present, on their displays, as specified by the authority having jurisdiction.

An ATS system may also include a means to control and limit movement authorities of CBTC-equipped trains operating in CBTC territory. CBTC movement authority limits shall be capable of being displayed on the ATS user interface, and any uncommanded reductions of authority limits shall be alarmed. For trains

operated with crews, movement authority limits may also be indicated to the train operator and/or conductor on their displays, as specified by the authority having jurisdiction.

6.3.5 Automatic train regulation

6.3.5.1 Schedule/headway regulation

An ATS system may have the capability to automatically monitor and regulate the performance of CBTC-equipped trains operating in CBTC territory, in relation to schedule and/or headway adherence.

An ATS system may include an automatic dispatching function (based on train identities, CBTC train location reports, scheduled and actual headways between trains, and service strategies implemented by authorized ATS users).

Schedule and headway regulation for CBTC-equipped trains shall be by means of dwell time variance (including train holds) and may also be by control of run times between stations (e.g., through adjustments to train acceleration and service brake rates, and speeds), as specified by the authority having jurisdiction. For trains operated with crews, the desired station departure time and desired speed profile between stations may be indicated to the train operator and/or conductor on their displays and, when operating in ATO mode, shall be implemented automatically by a CBTC system using the automatic speed regulation function of 6.2.1.

An ATS system may provide the capability to adjust the train service braking profiles for CBTC-equipped trains (e.g., in response to wet rail conditions). A CBTC system shall coordinate implementation of requested changes in service braking profiles to avoid conditions that would result in an emergency brake application.

6.3.5.2 Junction management

An ATS system may include automatic train regulation functions, based on CBTC train location reports, to facilitate appropriate train meets (such as transfers between local and express tracks, and at the merge point between different lines) in order to minimize overall system delays.

6.3.5.3 Energy optimization

An ATS system may have the capability to implement energy optimization algorithms for CBTC-equipped trains through the real-time control and coordination of train acceleration, train coasting, and train braking. The priority given to energy optimization versus schedule/headway regulation shall be as specified by the authority having jurisdiction.

6.3.6 Station stop functions

6.3.6.1 Stop train at next station

An ATS system may include the means to direct a single CBTC-equipped train or a group of CBTC-equipped trains to stop at the next station, even if the train is scheduled to bypass that station. For trains operated with crews, a CBTC system may indicate the ATS train stop information to the train operator and conductor on their displays. In ATO mode, a CBTC-equipped train shall automatically stop at the next station.

6.3.6.2 Hold train at station

For trains operated without crews, an ATS system shall include facilities to hold (and subsequently release) a CBTC-equipped train at a station.

For trains operated with crews, this function is optional and shall be as specified by the authority having jurisdiction. If this function is provided, a CBTC system may indicate the train hold information to the train operator and conductor on their displays, and/or prevent a CBTC-equipped train from departing the station in ATO mode.

6.3.6.3 Skip station stop

An ATS system may include facilities to direct a CBTC-equipped train or group of CBTC-equipped trains to pass through a station or group of stations without stopping. For trains operated with crews, a CBTC system may indicate the skip station information to the train operator and conductor on their displays. In ATO mode, the train shall automatically skip the designated stations.

6.3.6.4 Door control inhibit

An ATS system may include facilities to inhibit (and subsequently permit) CBTC control of the train doors, in accordance with 6.2.3.

6.3.7 Restricting train operations

The application and removal of the following functions can potentially introduce system hazards and the specific implementation of these functions shall be considered in the hazard analyses required by 5.3.2.

6.3.7.1 Stopping a train en route

An ATS system shall provide a means to stop a single CBTC-equipped train or group of CBTC-equipped trains immediately. A CBTC system shall initiate an immediate brake application on the designated trains and notify the train operator and conductor, if present, via their displays.

6.3.7.2 Temporary speed restrictions

An ATS system shall include facilities to impose (and remove) temporary speed restrictions for CBTC-equipped trains operating on any section of track in CBTC territory (see 6.1.3).

6.3.7.3 Switch/track blocking

An ATS system shall include facilities to block (and subsequently unblock) a switch, an exit signal, a route entry point, or a section of track within CBTC territory. A CBTC system shall prohibit CBTC-equipped trains from receiving movement authorities over blocked switches not aligned in the required position or into routes and/or sections of track that have been blocked (see 6.1.2 and 6.1.3).

6.3.7.4 Work zones

An ATS system shall include facilities to establish (and subsequently remove) temporary work zones for the protection of work crews and work trains.

A CBTC system shall enforce restricted speeds on approach to and through defined work zones (see 6.1.13). For trains operated with crews, information indicating that the restriction is due to a work zone shall be displayed to the train operator and conductor on their displays, and the CBTC system may preclude ATO mode of operation through a work zone.

An ATS system may also provide methods of visually and audibly indicating the approach and direction of trains along the wayside to warn on-track roadway workers in areas where visibility is restricted.

6.3.8 Passenger information system interfaces

An ATS system may interface with wayside and/or train-borne passenger information systems to trigger automatic passenger information messages, such as train arrival information, based on CBTC train location reports. Train-borne passenger information system interfaces shall be in accordance with IEEE Std 1477-1998.

6.3.9 Fault reporting

6.3.9.1 CBTC fault reporting

Failures and out-of-tolerance conditions detected by, or input to, a CBTC system that can impact the on-time performance of the transit system or result in some other loss of specific CBTC functionality may be automatically indicated on the ATS user interface display. Any alarms shall be categorized and prioritized into critical and noncritical alarms and logged. All critical alarms shall require acknowledgment.

6.3.9.2 Train fault reporting

Train-borne CBTC equipment may include interfaces to train-borne subsystems for the purposes of communicating train health data to the wayside for display on the ATS user interface displays, as specified by the authority having jurisdiction.

6.4 Interoperability interface requirements

This performance and functional requirements standard does not include interface design standards for interoperability. Where interoperability requirements are specified by the authority having jurisdiction, it shall be the responsibility of that authority to define the required interoperability interface standards.

NOTE—Examples of interoperability requirements include the following:

- Trains equipped with CBTC equipment furnished by one supplier to be capable of operating in CBTC territory equipped with wayside CBTC equipment furnished by another supplier
- Wayside equipment furnished by two separate suppliers to communicate with each other in the overlap area and with common central ATS equipment
- A basic operating unit with train-borne CBTC equipment furnished by one supplier to be capable of operating within a train with another basic operating unit equipped with train-borne CBTC equipment furnished by another supplier

A future CBTC standard may establish interoperability interface requirements.

Annex A

(informative)

Bibliography

[B1] American Public Transit Association's Manual for the Development of Rail Transit System Safety Program Plans, APTA Rail Safety Audit Program, June 1, 1989.

[B2] AREMA Communications & Signals Manual of Recommended Practices, 2004[7]

— Section 2, Railway Signal Systems
— Section 3.1.10, Recommended Functional/Operational Guidelines for Interconnection Between Highway Traffic Signals and Highway-Rail Grade Crossing Warning Systems
— Section 16, Vital Circuit and Software Design
— Section 17.1.1, Definition of Terms Used in the Manual Parts in Section 17
— Section 17.3.1, Recommended Safety Assurance Program for Electronic/Software-Based Products Used in Vital Signal Applications
— Section 17.3.3, Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications
— Section 17.3.5, Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications

[B3] ASCE 21-96 (Rev 1997), Automated People Mover Standards—Part 1.[8]

[B4] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition.[9]

[7]AREMA publications are available from the American Railway Engineering and Maintenance-of-Way Association, 8201 Corporate Drive, Suite 1125, Landover, MD 20785-2230 USA (www.arema.org/).

[8]ASCE standards are available from the American Society of Civil Engineers, 1015 15th Street NW, Suite 600, Washington DC 20005 USA (www.asce.org/).

[9]IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

Annex B

(informative)

Example functional block diagram for a typical CBTC system

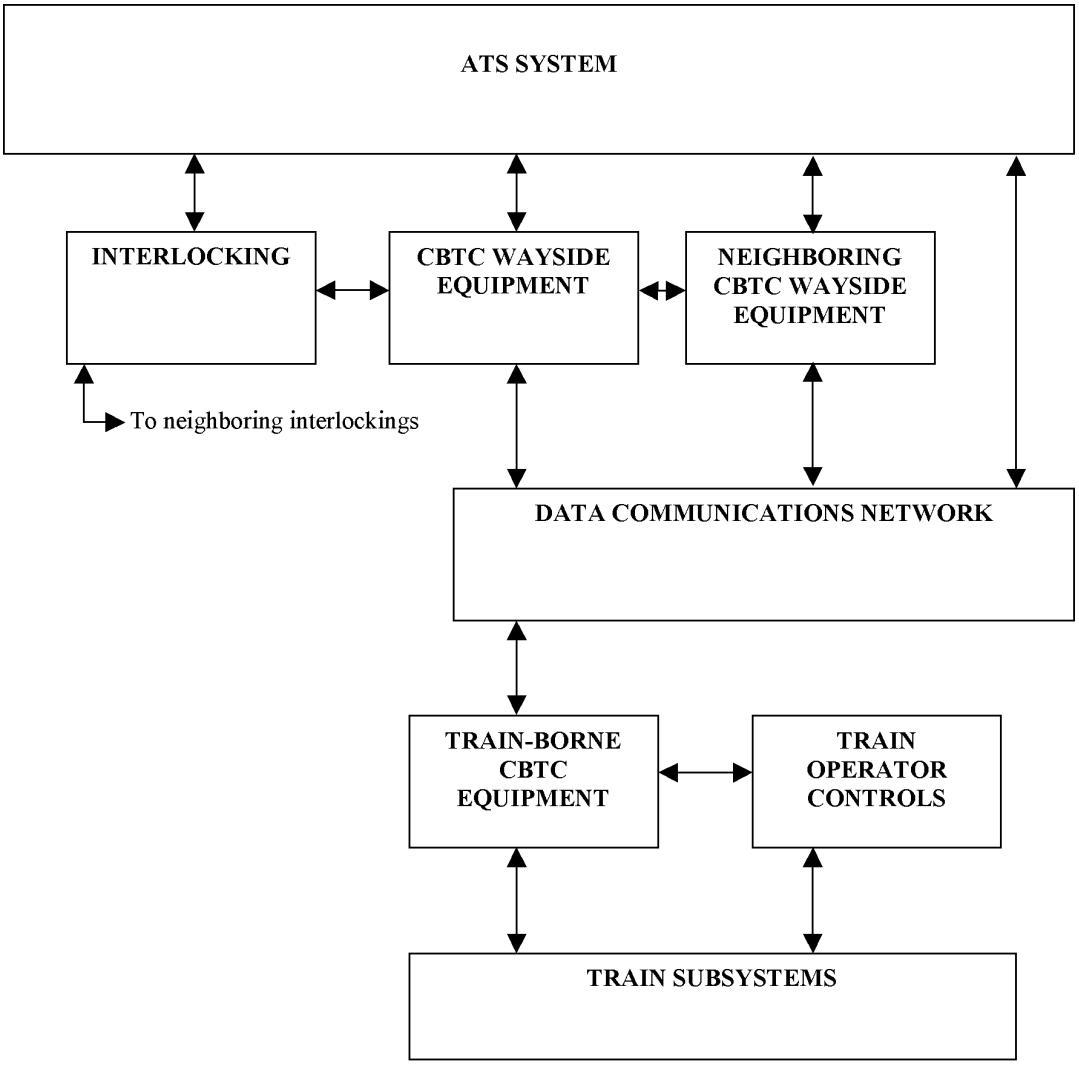

Figure B.1—Example functional block diagram for a typical CBTC system

Annex C

(informative)

Typical CBTC parameters

Table C.1 provides typical ranges for certain CBTC parameters for general guidance only. Parameter values for a specific application and/or a specific CBTC system design should be established by the authority having jurisdiction and/or the supplier, with due consideration of all relevant factors for the specific application.

Table C.1—Typical CBTC parameters

Parameter	Typical range
Maximum number of trains that can be processed by a single wayside controller	10 to 40 trains
Resolution of measured train location (i.e., as reported to establish movement authority limits for a following train for ATP purposes)	± 0.25 m to ± 6.25 m (± 10 in to ± 20 ft)
Accuracy of measured train location during normal (non-degraded) operations (i.e., maximum error in reported train location for ATP purposes)	± 5 m to ± 10 m (± 16 ft to ± 33 ft)
Accuracy of measured train location for programmed station stop (ATO) purposes—without platform edge doors	± 0.25 m (± 10 in)
Accuracy of measured train location for programmed station stop (ATO) purposes—with platform edge doors	± 0.05 m (± 2 in)
Resolution of train movement authority limits	± 0.25 m to ± 6.25 m (± 10 in to ± 20 ft)
Resolution of train speed measurement for ATP purposes	± 0.5 km/h to ± 2 km/h (± 0.3 mi/h to ± 1.25 mi/h)
Accuracy of train speed measurement for ATP purposes	± 3 km/h (± 2 mi/h)
Resolution of train speed commands (e.g., civil speed limits)	±0.5 km/h to ± 5 km/h (± 0.3 mi/h to ± 3 mi/h)
Train-to-wayside message communication delays	0.5 s to 2 s (nominal)
Wayside-to-train message communication delays	0.5 s to 2 s (nominal)
Wayside CBTC equipment reaction times	0.07 s to 1 s (nominal)
Train-borne CBTC equipment reaction times	0.07 s to 0.75 s (nominal)
Rollback detection criteria	0.5 m to 2 m (± 20 in to ± 6.5 ft)
Zero speed detection criteria	< 1 km/h to <3 km/h for 2 s (< 0.6 mi/h to < 2 mi/h for 2 s)

Annex D

(informative)

Typical safe braking model

D.1 Introduction

A typical safe braking model for CBTC systems is illustrated in Figure D.1.

It should be noted that Figure D.1 is not drawn to scale, but is a simplistic representation to assist in the understanding of a typical CBTC safe braking model. It should also be noted that the safe braking model outlined here is defined for level tangent track and would need to be adjusted for grades.

In Figure D.1, the *emergency brake curve* is the worst-case, open-loop, speed/distance curve a train will follow once the ATP has initiated an emergency brake application. This emergency brake curve must always be less than or equal to the *safe speed curve,* where *safe speed* is defined as the speed above which a critical hazard (derailment or collision) could occur.

In this model, safety factors are accounted for in the emergency brake curve, train position uncertainties, and other additional measurement tolerances incorporated in the CBTC system design, and there is no requirement to add additional safety margins.

The *ATP overspeed detection curve* is the speed-distance curve that the ATP subsystem uses to immediately initiate an emergency brake application, if the ATP subsystem detects that the measured speed exceeds this curve at the measured train location. When the ATP subsystem has initiated an emergency brake application, the ATP subsystem is no longer in the control loop, and the train will emergency brake at or below the emergency brake curve. The emergency brake curve includes an initial *propulsion runaway* period, until propulsion is disabled.

The *ATP profile curve* is the speed-distance curve that is an *ATP overspeed allowance* below the ATP overspeed detection curve. The ATP profile is the base curve used by the ATP subsystem.

D.2 Train-borne CBTC response time (A)

In Figure D.1, it is assumed that the CBTC system will measure the train speed and train location (relative to its movement authority limit) and compare the measure speed with the ATP profile speed at that measure location, every *A* seconds (worst case).

In Figure D.1, point X represents the situation where the CBTC measured speed is just below the ATP overspeed detection curve at the ATP measure location, i.e., although the ATP measured speed is above the ATP profile, it is still within the ATP overspeed allowance. As such, the CBTC system will not initiate emergency braking.

However, because of worst-case speed and location measurement errors (position uncertainty), it is possible that the actual speed and actual location of the train could be a point Y.

At this point in time, although the train operator and/or ATO subsystem would normally be attempting to bring the train speed down to the ATP profile speed, it is assumed that a failure occurs that results in the train accelerating rather than braking.

A seconds later, this situation will be detected by the CBTC system (point Z in Figure D.1), as the CBTC measured speed will now clearly be in excess of the ATP overspeed detection curve, and the CBTC system will immediately initiate an open-loop emergency brake application.

The speed at point Z therefore represents the maximum speed that a train can achieve above the ATP profile due to CBTC system's worst-case response times and measurement errors.

At this point, the remaining contributions to the safe braking model are determined by the vehicle characteristics only.

D.3 Propulsion disable response time (B)

During this component of the safe braking model (labeled B in Figure D.1), the train continues to accelerate until the train propulsion system has been disabled in response to the CBTC system initiating an emergency brake application.

D.4 Coast time (C)

During this component of the safe braking model (labeled C in Figure D.1), the train is assumed to be coasting at the maximum speed achieved as a result of the train accelerating prior to propulsion being disabled. This component of the safe braking model ends when emergency braking begins to take effect.

D.5 Emergency brake build-up time (D)

During this component of the safe braking model (labeled D in Figure D.1), the emergency brake rate will build up from zero to at least the GEBR.

D.6 Emergency braking at GEBR (E)

During this component of the safe braking model (labeled E in Figure D.1), the train continues to decelerate at the GEBR until the train comes to zero speed.

Note—The components D and E may be integrated into an equivalent single brake curve.

D.7 Position uncertainty

The safe braking model must include the maximum distance due to measurement inaccuracy by the CBTC system for both the leading and following train.

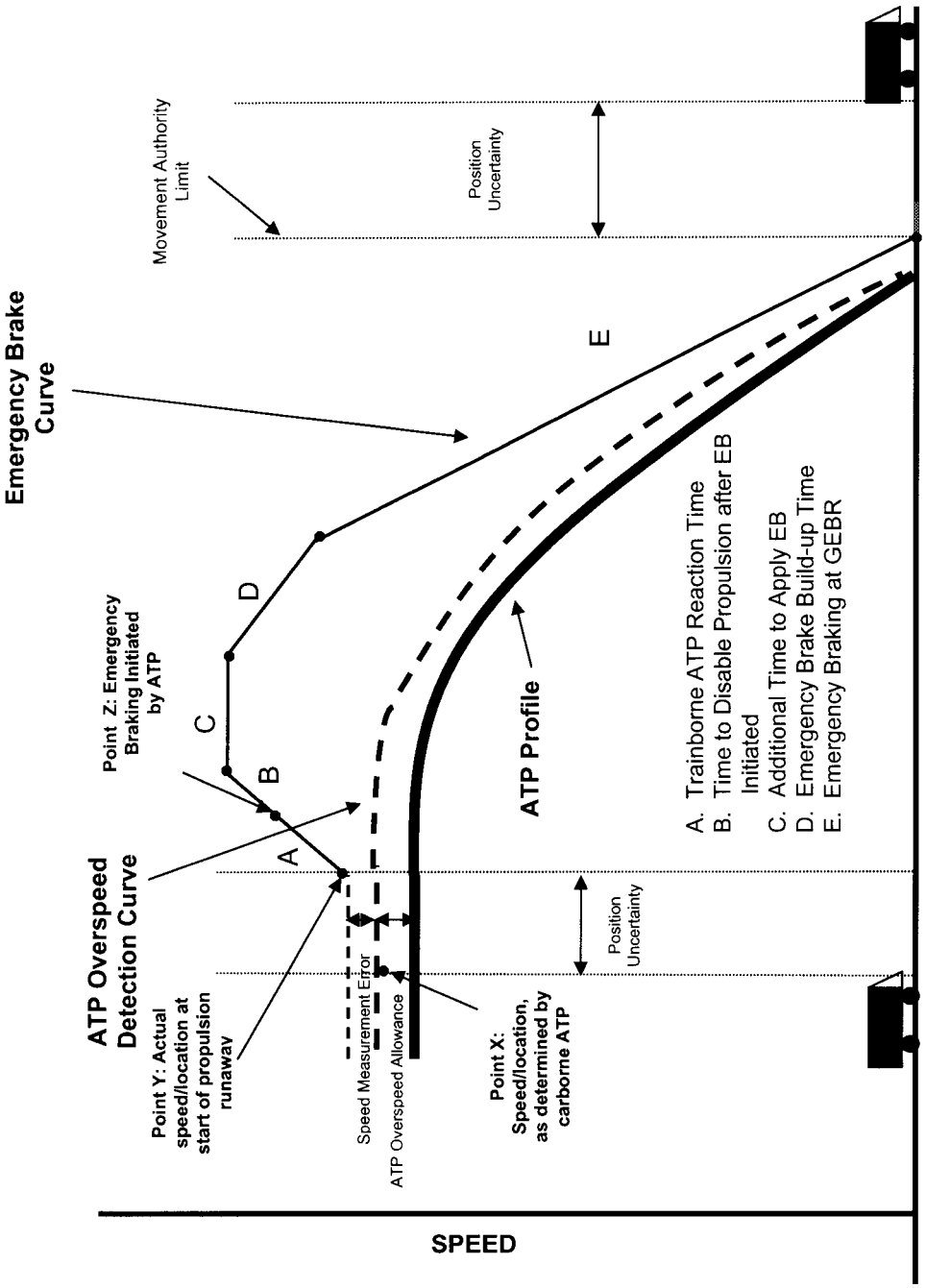

Figure D.1—Typical safe braking model

Annex E

(normative)

System Safety Program requirements

E.1 System Safety Program Plan (SSPP)

E.1.1 Purpose

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

E.1.2 Description

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

E.1.2.1 Program scope and objectives

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

a) Describe the scope of the overall program and the related System Safety Program.

b) List the tasks and activities of system safety management and engineering; describe the interrelationships between system safety and other functional elements of the program; list the other program requirements and tasks applicable to system safety, and identify where they are specified or described.

c) Account for all contractually required safety tasks and responsibilities. A matrix shall be provided to correlate requirements to the location in the SSPP where the requirement is addressed.

E.1.2.2 System safety organization

The SSPP shall describe the following:

a) The system safety organization or function within the organization of the total program using charts to show the organizational and functional relationships and lines of communication. It shall also show the organizational relationship between other functional elements having responsibility for tasks with system safety impacts and the system safety management and engineering organization. It shall identify the review and approval authority of applicable tasks by system safety.

b) The responsibility and authority of system safety personnel, other contractor organizational elements involved in the system safety effort, subcontractors, and system safety groups. It shall identify the methods by which safety personnel may raise issues of concern directly to the program manager or the program manager's supervisor within the corporation, the organizational unit responsible for executing each task, and the authority in regard to resolution of all identified hazards.

c) The staffing of the system safety organization for the duration of the contract to include manpower loading, control of resources, and a summary of the qualifications of key system safety personnel assigned to the effort, including those who possess coordination/approval authority for contractor prepared documentation.

d) The procedures by which the contractor will integrate and coordinate the system safety efforts, including assignment of the system safety requirements to action organizations and subcontractors, coordination of subcontractor System Safety Programs, integration of hazard analyses, program and design reviews, program status reporting, and system safety groups.

e) The process through which contractor management decisions will be made, including timely notification of unacceptable risks, necessary action, incidents or malfunctions, waivers to safety requirements, program deviations, etc.

f) Details of how resolution and action relative to system safety will be effected at the program management level possessing resolution authority.

E.1.2.3 System Safety Program milestones

The SSPP shall

a) Define System Safety Program milestones. It shall relate these to major program milestones, program element responsibility, and required inputs and outputs.

b) Provide a program schedule of safety tasks, including start and completion dates, reports, and reviews.

c) Identity subsystem, component, and software safety activities as well as integrated system level activities (i.e., design analyses, tests, and demonstrations) applicable to the System Safety Program, but specified in other engineering studies and development efforts to preclude duplication.

d) Provide the estimated manpower loading required to complete each task.

E.1.2.4 General system safety requirements and criteria

The SSPP shall describe the following:

a) General engineering requirements and design criteria for safety. It shall include safety requirements for support equipment and operational safety requirements for all appropriate phases of the life cycle up to, and including, disposal. It shall list the safety standards and system specifications containing safety requirements that shall be complied with, and include titles, dates, and where applicable, paragraph numbers.

b) Risk assessment procedures. It shall include the hazard severity categories, hazard probability levels, and the system safety precedence that shall be followed to satisfy the safety requirements of the program. It shall state any qualitative or quantitative measures of safety to be used for risk assessment, including a description of the acceptable/unacceptable risk levels, and include system safety definitions that modify, deviate from, or are in addition to those in this standard.

c) Closed-loop procedures for taking action to resolve identified unacceptable risk, including those involving nondevelopmental items.

E.1.2.5 Hazard analysis

The SSPP shall describe the following:

a) The analysis techniques and formats to be used in qualitative or quantitative analysis to identify hazards, their causes and effects, hazard elimination, or risk reduction requirements and how those requirements are met.

b) The depth within the system to which each technique is used, including hazard identification associated with the system, subsystem, components, software, hazardous materials, personnel, ground support equipment, nondevelopmental items, facilities and their interrelationship in the

logistic support, training, maintenance, operational, and disposal (including render safe and emergency disposal) environments.

c) The integration of subcontractor hazard analyses with overall system hazard analyses.

d) Efforts to identify and control hazards associated with materials used during the system's life cycle.

E.1.2.6 System safety data

The SSPP shall

a) Describe the approach for collecting and processing pertinent historical hazard data, mishap data, and safety lessons-learned data.

b) Identify deliverable data by title and number, and means of delivery (e.g., hard copy, electronically).

c) Identify nondeliverable system safety data and describe the procedures for accessibility by the authority having jurisdiction and retention of data of historical value.

E.1.2.7 Safety verification

The SSPP shall describe the following:

a) The verification (test, analysis, inspection, etc.) requirements for ensuring that safety is adequately demonstrated. It shall identify any certification requirements for software, safety devices, or other special safety features (e.g., render safe and emergency disposal procedures).

b) Procedures for making sure safety-related verification information is transmitted to the authority having jurisdiction for review and analysis.

c) Procedure for ensuring the safe conduct of all tests.

E.1.2.8 Audit program

The SSPP shall describe the techniques and procedures to be employed to make sure the objectives and requirements of the System Safety Program are being accomplished.

E.1.2.9 Training

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

E.1.2.10 Incident reporting

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

E.1.2.11 System safety interfaces

The SSPP shall identify, in detail, the following:

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

b) The interface between system safety and all system integration and test disciplines

E.2 Preliminary hazard analysis (PHA)

E.2.1 Purpose

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

E.2.2 Description

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

a) Hazardous components (e.g., fuels, propellants, lasers, toxic substances, hazardous construction materials, pressure systems, and other energy sources).

b) Safety-related interface considerations among various elements of the system (e.g., material compatibilities, electromagnetic interference, inadvertent activation, fire/explosive initiation and propagation, and hardware and software controls). This shall include consideration of the potential contribution by software (including software developed by other contractors/sources) to subsystem/system mishaps. Safety design criteria to control safety-critical software commands and responses (e.g., inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or other designated undesired events) shall be identified and appropriate action taken to incorporate them in the software (and related hardware) specifications.

c) Environmental constraints, including the operating environments (e.g., drop, shock, vibration, extreme temperatures, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects).

d) Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (e.g., human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors, such as equipment layout, lighting requirements, potential exposures to toxic materials; effects of noise or radiation on human performance). Those test-unique hazards that will be a direct result of the test and evaluation of the article or vehicle.

e) Facilities, real property installed equipment, support equipment (e.g., provisions for storage, assembly, checkout, proof/testing of hazardous systems/assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials/wastes; radiation or noise emitters; electrical power sources), and training (e.g., training and certification pertaining to safety operations and maintenance).

f) Safety-related equipment, safeguards, and possible alternate approaches (e.g., interlocks; system redundancy; fail-safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers).

g) Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and /or design changes developed.

E.3 Subsystem hazard analysis (SSHA)

E.3.1 Purpose

The SSHA shall verify subsystem compliance with safety requirements contained in subsystem specifications and other applicable documents; identify previously unidentified hazards associated with the design of subsystems, including component failure modes, critical human error inputs, and hazards resulting from functional relationships between components and equipment comprising each subsystem; recommend actions necessary to eliminate identified hazards or control their associated risk to acceptable levels.

E.3.2 Description

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

The analysis shall include a determination

a) Of the modes of failure, including reasonable human errors as well as single-point and common-mode failures, and the effects on safety when failures occur in subsystem components.
b) Of potential contribution of hardware and software (including that which is developed by other contractors/sources) events, faults, and occurrences (such as improper timing) on the safety of the subsystem.
c) That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.
d) That the method of implementation of hardware, software, and facilities design requirements and corrective actions has not impaired or decreased the safety of the subsystem nor has it introduced any new hazards or risks.
e) Of the implementation of safety design requirements from top level specifications to detailed design specifications for the subsystem. The implementation of safety design requirements developed as part of the PHA shall be analyzed to ensure that it satisfies the intent of the requirements.
f) Of test plan and procedure recommendations to integrated safety testing into the hardware and software test programs.
g) That system level hazards attributed to the subsystem are analyzed and that adequate control of the potential hazard is implemented in the design.

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

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

E.4 System hazard analysis (SHA)

E.4.1 Purpose

The SHA shall

a) Verify system compliance with safety requirements contained in system specifications and other applicable documents.

b) Identify previously unidentified hazards associated with the subsystem interfaces and system functional faults.

c) Assess the risk associated with the total system design, including software, and specifically of the subsystem interfaces.

d) Recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

E.4.2 Description

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

This analysis shall include a review of subsystem interrelationships for the following:

a) Compliance with specified safety design criteria

b) Possible independent, dependent, and simultaneous hazardous events including systems failures; failures of safety devices; common cause failures and events; and system interactions that could create a hazard or result in an increase in mishap risk

c) Degradation in the safety of a subsystem or the total system from normal operation of another subsystem

d) Design changes that affect subsystems

e) Effects of reasonable human errors

f) Determination

   1) Of potential contribution of hardware and software (including that which is developed by other contractors/sources, or commercial off-the-shelf hardware or software) events, faults, and occurrences (such as improper timing) on safety of the system.

   2) That the safety design criteria in the hardware, software, and facilities specification(s) have been satisfied.

   3) That the method of implementation of the hardware, software, and facilities design requirements and corrective actions has not impaired or degraded the safety of the system nor has it introduced any new hazards.

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

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

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

E.5 Operating and support hazard analysis (O&SHA)

E.5.1 Purpose

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

E.5.2 Description

An O&SHA shall be performed and documented to examine procedurally controlled activities. The O&SHA identifies and evaluates hazards resulting from the following:

- The implementation of operations or tasks performed by persons, considering the planned system configuration/state at each phase of activity
- The facility interfaces; the planned environments (or ranges thereof)
- The supporting tools or other equipment, including software controlled automatic test equipment, specified for use; operational/task sequence, concurrent task effects and limitations
- The potential for unplanned events, including hazards introduced by human errors

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

The analysis shall identify the following:

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

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

The contractor shall update the O&SHA as a result of any system design or operational changes.

E.6 Risk assessment

The hazard resolution process shall be initiated by defining the physical and functional characteristics of the 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:

a) Data from previous accidents or operating experience
b) Expert opinion and hazard scenarios

c) Checklists of potential hazards

d) Previous hazard analyses

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

1) Design to eliminate hazards

2) Design to control hazards

3) Use safety devices

4) Use warning devices

5) Implement special procedures

6) Accept the hazard

7) Eliminate the system/subsystem/equipment

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

Table E.1 provides an example of the relationship between risk, severity, and probability as it may be applied when assessing CBTC systems. The authority having jurisdiction may choose to modify this table to reflect existing procedures or requirements.

Table E.1—Risk assessment

	Hazard severity			
Frequency of occurrence	**1—Catastrophic**	**2—Critical**	**3—Marginal**	**4—Negligible**
A—Frequent	Unacceptable (1A)	Unacceptable (2A)	Unacceptable (3A)	Undesirable (4A)
B—Probable	Unacceptable (1B)	Unacceptable (2B)	Undesirable (3B)	Acceptable with review (4B)
C—Occasional	Unacceptable (1C)	Unacceptable (2C)	Acceptable with review (3C)	Acceptable with review (4C)
D—Remote	Unacceptable (1D)	Unacceptable (2D)	Acceptable with review (3D)	Acceptable without review (4D)
E—Improbable	Undesirable (1E)	Undesirable (2E)	Acceptable without review (3E)	Acceptable without review (4E)

Residual risk levels

Unacceptable (1A/B/C/D, 2A/B/C/D, and 3A)

CBTC systems with residual risks rated at this level are considered unacceptable; hazards must be mitigated through fail-safe designs.

Undesirable (1E, 2E, 3B, and 4A)

CBTC systems with residual risks rated at this level are considered undesirable; depending on economic and functional requirements, CBTC systems with hazards rated at this risk level may be considered acceptable with explicit agreement from the authority having jurisdiction.

Acceptable with review (3C/D and 4B/C)

CBTC systems with residual risks rated at this level are considered acceptable with review; depending on economic and functional requirements, CBTC systems with hazards rated at this risk level may be considered acceptable with notification to the authority having jurisdiction.

Acceptable without review (3E and 4D/E)

CBTC systems with residual risks rated at this level are considered acceptable without review; additional design effort or system revision is not required to reduce the severity or probability of hazards with this risk level.

Frequency of occurrence

A—Frequent	=	Likely to occur frequently; MTBHE is less than 1000 operating hours.
B—Probable	=	Will occur several times in the life of an item; MTBHE is equal to or greater than 1000 operating hours and less than 100 000 operating hours.
C—Occasional	=	Likely to occur some time in the life of an item; MTBHE is equal to or greater than 100 000 operating hours and less than 10 000 000 operating hours.
D—Remote	=	Unlikely, but possible to occur in the life of an item; MTBHE is equal to or greater than 10 000 000 operating hours and less than 1 000 000 000 operating hours.
E—Improbable	=	So unlikely, it can be assumed occurrence may not be experienced; MTBHE is equal to or greater than 1 000 000 000 operating hours.

Hazard severity

1—Catastrophic	=	Fatality, system loss, or severe environmental damage.
2—Critical	=	Severe injury, severe occupational illness, major system or environmental damage.
3—Marginal	=	Minor injury, minor occupational illness, or minor system or environmental damage.
4—Negligible	=	Less than minor injury, occupational illness, or less than minor system or environmental damage.

Annex F

(informative)

Typical approaches to specifying CBTC system availability

F.1 Traditional *equipment-based* approach

The traditional approach to defining system availability is the probability that the system is capable of operating and performing its intended function at a random point in time, as determined by the system MTBFF and MTTRS, as shown in Equation (F.1):

$$\text{CBTC system availability} = \text{system MTBFF} / (\text{system MTBFF} + \text{system MTTRS}) \quad \text{(F.1)}$$

where

System MTTRS is the sum of the system MTTR and the mean travel times for maintenance personnel to travel to the site of a failure.

With this approach, the authority having jurisdiction would typically specify the following:

a) The quantitative CBTC system availability requirements
b) The average travel times to be assumed for maintenance personnel to travel to the site of a failure
c) The boundaries of the CBTC system covered by the availability requirement
d) The type of CBTC failures to be included in defining the system MTBFF

For a given CBTC system configuration, the predicted CBTC system availability could be determined analytically from estimates of subsystem MTBFFs and MTTRs.

Actual CBTC system availability could be determined from measurements of actual in-service system MTBFF and MTTRS, with appropriate adjustments for factors that are not included within the specified boundaries of the CBTC system.

F.2 Alternative *delayed trip-based* approach

An alternative approach is to define CBTC system availability in terms of the system's contributions to the desired on-time performance of the transit system, as shown in Equation (F.2):

$$\text{CBTC system availability} = \frac{1 - \Sigma w_x \text{Revenue trips delayed more than } t_x \text{ by CBTC Type failure}}{\text{Total scheduled revenue trips}} \quad \text{(F.2)}$$

where

Revenue trip is a scheduled movement of a train, of defined length, from a point of origin to a destination,
t_x is a defined delay threshold,
w_x is a weighting factor associated with that delay threshold.

With this approach, CBTC system availability would take into account the delays experienced by passengers. As the passenger judges transit system availability on the basis of the wait and travel time variations of the service provided, CBTC system failures that result in longer delays are penalized with a

greater weighting factor than failures that result in shorter delays. In general, delay thresholds would be related to the operating headways, as delays at shorter headways impact on-time performance more significantly.

The CBTC system availability requirement may also consider other failure types, to the extent that such failures impact fleet availability. For example, even if a train-borne CBTC equipment failure does not immediately impact the on-time performance of the transit system, it may subsequently result in missed revenue trips if the failure repair time results in the train being unavailable for service.

With this approach, the authority having jurisdiction would typically specify the following:

a) The quantitative CBTC system availability requirements
b) The various delay thresholds and weighting factors
c) The average travel times to be assumed for maintenance personnel to travel to the site of a failure
d) The boundaries of the CBTC system covered by the availability requirements
e) The type of CBTC failures to be included in defining the system availability

For a given CBTC system configuration, the predicted CBTC system availability could be determined through computer modeling from estimates of subsystem MTBFFs and MTTRs, and an assumed system operating plan.

Actual CBTC system availability could be determined from measurements of actual in-service delays, with appropriate adjustments for factors that are not included within the specified boundaries of the CBTC system.