



Norfolk Southern Corporation
1200 Peachtree Street, N.E.
Atlanta, Georgia, 30309

September 15, 2006

Ms. Jo Strang
Associate Administrator for Safety

Mr. Grady Cothen
Deputy Associate Administrator for Safety
Standards and Program Development

Federal Railroad Administration
1120 Vermont Avenue, N.W.- Mail Stop 25
Washington, DC 20590

RE: Title 49 CFR Part 236, Subpart H §236.905 (c)

Dear Ms. Strang and Mr. Cothen:

Attached is the Norfolk Southern Railroad Safety Program Plan (RSPP). This document is being submitted for FRA approval as required by Title 49 CFR Part 236, subpart H §236.905 (c). As required, this petition and the RSPP document are being submitted in triplicate.

The primary contact at Norfolk Southern during the review of this petition is:

Tom Schnautz
Manager Centralized Train Control Systems
1200 Peachtree St., N.E.- Box 123
Atlanta, GA 30309
(404) 527-2888
Tom.Schnautz@nscorp.com

We look forward to your review and approval. Please let me know if you have any questions or require additional information.

Sincerely,


Tom W. Schnautz
Mgr. Centralized Train Control Systems
Norfolk Southern Railway



Railroad Safety Program Plan (RSPP)

Submitted in fulfillment of 49 C.F.R. § 236.905

Version 2.0

September 2006

This Page Intentionally Left Blank

Revision History

Date	Revision	Description	Author
9/11/06	2.0	Formal FRA Submission	TWS

Table of Contents

<u>1. INTRODUCTION AND OVERVIEW</u>	<u>7</u>
1.1 INTRODUCTION.....	7
1.2 GOALS AND OBJECTIVES	8
1.3 APPLICABILITY.....	8
1.4 DOCUMENT OVERVIEW	9
<u>2. APPLICABLE DOCUMENTS</u>	<u>11</u>
<u>3. RAILROAD SAFETY PROGRAM PLAN REQUIREMENTS [49 C.F.R. § 236.905]</u>	<u>13</u>
3.1 REQUIREMENTS AND CONCEPTS [49 C.F.R. § 236.905 (B) (1)].....	13
3.1.1. METHODS TO EVALUATE BEHAVIOR [49 C.F.R. § 236.905 (B) (1) (I)]	14
3.1.2. RISK ASSESSMENT PROCEDURES [49 C.F.R. § 236.905 (B) (1) (II)]	15
3.1.3. SYSTEM SAFETY PRECEDENCE [49 C.F.R. § 236.905 (B)(1)(III)]	17
3.1.4. SAFETY ASSESSMENT PROCESS REQUIREMENTS [49 C.F.R. § 236.905 (B)(1)(IV)]	18
3.2 DESIGN FOR VERIFICATION AND VALIDATION (V&V) [49 C.F.R. § 236.905 (B) (2)]	20
3.2.1. METHODOLOGY.....	20
3.2.2. STANDARDS.....	20
3.2.3. DOCUMENTATION.....	21
3.2.4. INDEPENDENT REVIEW AND ASSESSMENT OF VERIFICATION AND VALIDATION	21
3.3 DESIGN FOR HUMAN FACTORS [49 C.F.R. § 236.905 (B)(3)].....	22
3.4 CONFIGURATION MANAGEMENT CONTROL PLAN [49 C.F.R. § 236.905(B) (4)].....	22
3.5 RAILROAD SAFETY PROGRAM PLAN MODIFICATIONS [§ 236.905(D)]	24
<u>4. PRODUCT SAFETY PLAN (PSP) [49 C.F.R. § 236.907]</u>	<u>25</u>
4.1 DESCRIPTION OF THE PRODUCT [49 C.F.R. § 236.907 (A)(1)].....	25
4.2 DESCRIPTION OF RAILROAD OPERATIONS [49 C.F.R. § 236.907 (A)(2)]	26
4.3 OPERATIONAL CONCEPTS DOCUMENT [49 C.F.R. § 236.907 (A)(3)].....	26
4.4 SAFETY REQUIREMENTS DOCUMENT [49 C.F.R. § 236.907 (A)(4)]	27
4.5 PRODUCT ARCHITECTURE DOCUMENT [49 C.F.R. § 236.907 (A)(5)]	27
4.6 HAZARD LOG [49 C.F.R. § 236.907 (A)(6)]	27
4.7 RISK ASSESSMENT REQUIREMENTS [49 C.F.R. § 236.907 (A) (7)]	28
4.8 HAZARD MITIGATION ANALYSIS [49 C.F.R. § 236.907 (A) (8)].....	28
4.9 SAFETY ASSESSMENT AND V&V PROCESS [49 C.F.R. § 236.907 (A) (9)].....	29
4.10 SAFETY ASSURANCE CONCEPTS [49 C.F.R. § 236.907 (A) (10)]	29
4.11 HUMAN FACTORS ANALYSIS [49 C.F.R. § 236.907 (A) (11)]	30
4.12 TRAINING REQUIREMENTS [49 C.F.R. § 236.907 (A) (12)]	30
4.13 TEST PROCEDURES AND EQUIPMENT [49 C.F.R. § 236.907 (A) (13)].....	31
4.14 APPLICABILITY TO OTHER RULES AND REGULATIONS [49 C.F.R. 236.907 (A) (14)].....	31
4.15 SECURITY MEASURES FOR THE PRODUCT [49 C.F.R. § 236.907 (A) (15)]	32

4.16	WARNINGS AND WARNING LABELS [49 C.F.R. § 236.907 (A) (16)].....	32
4.17	IMPLEMENTATION TESTING [49 C.F.R. § 236.907 (A) (17)].....	32
4.18	POST IMPLEMENTATION TESTING AND MONITORING PROCEDURES [49 C.F.R. § 236.907 (A) (18)]	33
4.19	SAFETY-CRITICAL ASSUMPTIONS [49 C.F.R. § 236.907 (A) (19)]	33
4.20	INCREMENTAL AND PREDEFINED CHANGES [49 C.F.R. § 236.907 (A) (20)].....	34
4.21	COMMUNICATION OF HAZARDS [§ 236.907(D)].....	34
5.	<u>MINIMUM PERFORMANCE STANDARD [49 C.F.R. § 236.909].....</u>	35
5.1	PERFORMANCE STANDARD FOR SAFETY RISK MANAGEMENT [§ 236.909(A) AND (B)].....	35
5.2	PERFORMANCE STANDARD FOR SAFETY RISK MEASUREMENT [§ 236.909(A) AND (B)]	35
5.3	RISK ASSESSMENT SCOPE [§ 236.909(C) AND (D)].....	35
5.4	RISK ASSESSMENT GENERAL PRINCIPLES [§ 236.909(E) (2) AND (3)]	36
5.5	MONITORING OF OPERATIONAL SERVICE [49 C.F.R. §§ 236.917 (B) 236.907 (A)]	37
6.	<u>PSP REVIEW AND APPROVAL [49 C.F.R. §236.913].....</u>	38
6.1	RAILROAD REVIEW AND APPROVAL OF PSP [49 C.F.R. § 236.913 (C) - (E)].....	38
7.	<u>IMPLEMENTATION AND OPERATION [49 C.F.R. § 236.915]</u>	39
7.1	COMPLIANCE WITH PSP AND RSPP REQUIREMENTS [49 C.F.R. § 236.915 (A), (B)].....	39
7.2	RESTRICTIONS ON TESTING [49 C.F.R. § 236.915 (C)].....	39
7.3	SYSTEM OR SUBSYSTEM FAILURES [49 C.F.R. § 236.915 (D)]	39
8.	<u>OPERATIONS AND MAINTENANCE MANUAL [49 C.F.R. § 236.919].....</u>	40
9.	<u>TRAINING AND QUALIFICATION PROGRAM [49 C.F.R. §§ 236.921 - 236.929]</u>	41
10.	<u>HUMAN-MACHINE INTERFACE [49 C.F.R. PART 236, APPENDIX E]</u>	42
11.	<u>APPENDIX A – APPLICABLE SYSTEMS</u>	44
12.	<u>APPENDIX B – HAZARD IDENTIFICATION AND MITIGATION</u>	45
B.1	PRELIMINARY HAZARDS ANALYSIS (PHA)	45
B.2	FUNCTIONAL FAULT TREE (FFT).....	46
B.3	SUBSYSTEM HAZARD ANALYSIS (SSHA)	47
B.4	OPERATING & SUPPORT HAZARD ANALYSIS (O&SHA)	47

13. APPENDIX C – SAFETY VERIFICATION AND VALIDATION [49 C.F.R. PART 236, APPENDIX C]..... 48

C.1 VERIFICATION ACTIVITIES.....	48
C.1.1. FAULT TREE ANALYSIS.....	48
C.1.2. FAILURE MODES AND EFFECTS ANALYSIS	49
C.1.3. SOFTWARE V&V	49
C.1.4. FAULT HAZARD ANALYSIS	50
C.1.5. SAFETY VERIFICATION TESTING.....	50
C.1.6. VALIDATION ACTIVITIES	50

Glossary of Terms & Acronyms

The following abbreviations and acronyms are used in this document:

AREMA	American Railway Engineering and Maintenance of Way Association
CCB	Configuration Control Board
C.F.R.	Code of Federal Regulations
CM	Configuration Management
DoD	Department of Defense
FFT	Functional Fault Tree
FHA	Functional Hazard Assessment or Fault Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FOIA	Freedom of Information Act
FRA	Federal Railroad Administration
FTA	Fault Tree Analysis
HMI	Human Machine Interface
IEEE	Institute of Electrical and Electronics Engineers
MIL-STD	Military Standard
MTTHE	Mean Time to Hazardous Event
MTTR	Mean Time to Repair
NS	Norfolk Southern Railway
O&SHA	Operating & Support Hazard Analysis
OMM	Operations and Maintenance Manual
PHA	Preliminary Hazard Analysis
PSP	Product Safety Plan
RSPP	Railroad Safety Program Plan
SAE	Society of Automotive Engineers
SAP	Safety Assessment Process
SSHA	Subsystem Hazard Analysis
SSIHA	Subsystem Interface Hazard Analysis
V&V	Verification and Validation

The following definitions of terms are used in this document:

Component	An element, device or appliance that is part of a system or subsystem.
Developer	Any person or organization, internal or external to NS that performs development of any component or components to be used in a safety critical processor-based signal or train control system or subsystem.
Hazard	An existing or potential condition that may result in an accident.
High Degree Of Confidence	Credible safety analysis exists that is sufficient to persuade a reasonable decision maker that the likelihood of the changed condition associated with the new product being less safe than the existing condition is small.
Mean Time to Hazardous Event (MTTHE)	The average or expected time that a system, subsystem, or component will operate prior to the occurrence of an unsafe failure.
Previous Condition	Refers to the calculated risk inherent in the portion of the existing method of operation that is relevant to the change under analysis.
Processor-based signal and train control system	A product that is dependent on a digital processor(s) for its proper functioning.
Risk	An expression of the possibility/impact of a mishap in terms of hazard severity and hazard probability.
Risk Assessment	The process of determining, either quantitatively or qualitatively, the measure of risk associated with using the new processor-based signal or train control system, and/or of the previous condition.
Safety-critical	A term applied to a function, a system, or any portion thereof, the correct performance of which is essential to the safety of personnel and/or equipment, or the incorrect performance of which may cause a hazardous condition, or allow a hazardous condition to exist that should have been prevented by the function or system.
Subsystem	A defined portion of a system.
System	Refers to a processor-based signal and train control system,

safety-critical subsystem or safety-critical component thereof, as the context requires.

**System Safety
Precedence**

The order of precedence in which methods used to eliminate or control-identified hazards within a system is implemented.

Validation

A process for determining whether a product's design requirements fulfill its intended safety design objectives during its development and life cycle. The goal of the validation process is to determine if the correct product was built.

Verification

A structured and managed set of activities which identify the vital functions required to be performed by the system and demonstrate that the system, including its subsystems, interfaces, and components, implements the vital functions fail safely to a level that meets the allocated system safety goals. The goal of the safety verification activities is to determine if the product was built correctly.

1. Introduction and Overview

1.1 Introduction

This Railroad Safety Program Plan (RSPP) is Norfolk Southern Railway's (NS) strategic safety planning document for the development and implementation of safety-critical processor-based signal and train control systems.

This RSPP is not specific to any particular system design and implementation, but rather represents NS' plans to ensure safety during the implementation of any safety-critical processor-based signal or train control system. The RSPP is viewed as a living document that includes all aspects of product safety from design through implementation.

This RSPP is based on the requirements of the Federal Railroad Administration Rulemaking 49 C.F.R. Sections 209, 234 and 236 entitled "Standards for Development and Use of Processor-Based Signal and Train Control Systems" effective June 6, 2005 herein referred to as "Subpart H." Sections 1-2 provide an introduction and overview of the RSPP and a list of the applicable systems on NS. Section 3 of this RSPP provides NS requirements related to safety requirements and concepts, verification and validation, human factors, and configuration management employed by NS to meet safety goals for safety-critical processor-based signal and train control systems subject to the above mentioned rule. Sections 4 through 10 of the RSPP establish definitive requirements for a Product Safety Plan (PSP) that must be prepared for the implementation, operation, and maintenance of a safety-critical processor-based signal and train control system developed and installed on NS under "Subpart H."

A PSP must be prepared for each specific type of safety-critical processor-based signal or train control system (or safety-critical subsystem or component) deployed by the NS. The Product Developer shall prepare, with the assistance of NS, a PSP that is compliant with this RSPP and with applicable Federal regulations. NS will supply the required supporting data to assist in the authentication of the PSP. The PSP will become a NS document. The PSP is specific to a particular system design and implementation and represents both the developer's and NS's plans to ensure safety during the lifetime of a safety-critical processor-based signal and train control system. A PSP is viewed as a living document that must include all aspects of product safety throughout design, implementation, revision and decommissioning.

The principal burden for preparing a PSP will reside with the developer; however NS will provide assistance to the developer during the development. NS requirements for product development will be product specific, furnished to the Developer and will be listed in the PSP. The PSP must be compliant with this RSPP, other applicable NS rules and policies and applicable governmental regulations. Once approved by NS and FRA, the PSP will become a railroad document that tracks and demonstrates the safety of the safety-critical processor-based signal and train control equipment described in the PSP. All documentation supporting the safety-critical processor-based signal and train control system shall be available for inspection and replication by the FRA and/or FRA approved designee(s) in accordance with applicable regulation.

As part of a PSP submission, Developer or NS may include information that includes trade secrets or sensitive security information in which case such materials may be submitted in accordance with 49 C.F.R. § 209.11 (Request for confidential treatment), 49 C.F.R. Part 15 (Protection Of Sensitive Security Information) and the Freedom of Information Act (FOIA).

Section 6 identifies the NS requirements for notifying the FRA of its preparation of a PSP to ensure compliance with the procedures established in this RSPP.

1.2 Goals and Objectives

The overall goals for the deployment of any safety-critical processor-based signal and train control system on NS are to enhance safety and/or increase capacity and efficiency where the system is deployed. The objective of this RSPP is to ensure that the deployment of any safety-critical processor-based signal and train control system developed and implemented under the provisions of "Subpart H" does not result in a level of safety risk that exceeds the level of safety risk in the existing system.

The RSPP will provide a uniform requirement for developing and implementing a system safety program that can identify the hazards associated with a processor-based signal and train control system and impose design requirements and management controls to mitigate such hazards. The goal will be to eliminate hazards and/or reduce the risk related to the hazards to an acceptable level.

1.3 Applicability

This RSPP applies to safety-critical processor-based signal and train control systems, safety-critical subsystems or safety-critical components thereof, developed and implemented subject to the requirements of 49 CFR Part 236,

subpart H. This RSPP also applies to some highway-rail grade crossing warning systems that are covered under the rule as applicable and described in 234.275(a).

1.4 Document Overview

This document provides the NS requirements for safety, performance, design, development, verification and validation, human factors, implementation, configuration management, and maintenance to ensure the safe operation of safety-critical processor-based signal and train control systems. In addition, this RSPP establishes definitive requirements for any PSP developed for a safety-critical processor-based signal and train control system intended for deployment on NS. The following is an outline of the document:

- Section 1 describes the scope of the document.
- Section 2 lists applicable documents that are referenced in this RSPP.
- Section 3 presents the minimum safety requirements for the development of safety-critical processor-based signal and train control systems as defined in 49 C.F.R. § 236.905.
- Section 4 presents requirements for the development of PSPs as defined in 49 C.F.R. § 236.907.
- Section 5 defines the minimum performance standard for signal and safety-critical processor-based signal and train control systems as defined in 49 C.F.R. § 236.909.
- Section 6 delineates the review and approval process for the PSP as defined in 49 C.F.R. § 236.913.
- Section 7 contains requirements for the implementation and operation of safety-critical processor-based signal and train control systems as defined in 49 C.F.R. §236.915.
- Section 8 defines requirements for system operation and maintenance manuals as defined in 49 C.F.R. § 236.919.
- Section 9 defines training and qualification program requirements as delineated in 49 C.F.R. §§ 236.921, 236.923, 236.925, 236.927, and 236.929.
- Section 10 defines human-machine interface requirements as delineated in 49 C.F.R. Part 236, Appendix E.

-
- Appendix A provides a list of safety-critical processor-based signal and train control systems on NS subject to the provisions of 49 C.F.R. § 236 and this RSPP.
 - Appendix B describes NS recommended hazard identification methodologies and techniques for evaluating the proposed safety-critical processor-based signal and train control system safety concepts and designs and for establishing safety requirements.
 - Appendix C defines NS minimum safety V&V activity requirements.

2. Applicable Documents

The following documents were used in the preparation of this RSPP. These documents will be kept in a library at NS headquarters in Atlanta, Georgia.

- a) 49 CFR Part 236, Subpart H, "Standards for Development and Use of Processor-Based Signal and Train Control Systems; Final Rule" dated March 7, 2005.
- b) MIL-STD-882C, "System Safety Program Requirements" with Notice, 1 US DoD, 13 March 1996.
- c) IEEE STD 610.12-1990, "IEEE Standard Glossary of Software Engineering Terminology".
- d) IEEE STD 730.1-1998, "IEEE Guide for Software Quality Assurance Planning", the Institute of Electrical and Electronics Engineers, Inc., 1998.
- e) IEEE STD 828-1998, "IEEE Standard for Software Configuration Management", the Institute of Electrical and Electronics Engineers, Inc. 1998.
- f) IEEE STD 830-1998, "IEEE Recommended Practice for Software Requirements Specifications", the Institute of Electrical and Electronics Engineers, Inc. 1998.
- g) IEEE STD 982.1-1988, "IEEE Standard Dictionary of Measures to Produce Reliable Software", the Institute of Electrical and Electronics Engineers, Inc., 1989.
- h) IEEE STD 982.2-1988, "IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software", the Institute of Electrical and Electronics Engineers, Inc., 1989.
- i) IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation", IEEE Computer Society.
- j) IEEE STD 1016-1998, "IEEE Recommended Practice for Software Design Descriptions", IEEE Computer Society, 23 September 1998.
- k) IEEE STD 1028-1997, "IEEE Standard for Software Reviews, IEEE Computer Society, 4 March 1998.
- l) IEEE STD 1042-1987, "IEEE Guide to Software Configuration Management", IEEE Computer Society, 10 September 1987.
- m) IEEE STD 1058.1-1998, "IEEE Standard for Software Project Management Plans", the Institute of Electrical and Electronics Engineers, Inc., 1998.
- n) IEEE STD 1074-1997, "IEEE Standard for Developing Software Life Cycle Processes", the Institute of Electrical and Electronics Engineers, Inc., 1998.
- o) IEEE STD 1233, 1998 Edition, "IEEE Guide for Developing System Requirements Specifications", the Institute of Electrical and Electronics, Inc., 1998.

-
- p) IEEE STD 1483-2000, "IEEE Standard for Verification of Vital Function in Processor Based Systems Used in Rail Transit Control", IEEE Vehicular Technology Society, 30 March 2000.

3. Railroad Safety Program Plan Requirements [49 C.F.R. § 236.905]

This section sets safety requirements for safety-critical processor-based signal and train control systems subject to § 236 that may be developed, acquired, or installed by NS. In general, these requirements address:

1. The development of a preliminary safety analysis that includes:
 - a. Methods used to evaluate system behavior;
 - b. Risk assessment procedures;
 - c. The system safety precedence to be followed, and;
 - d. Safety assessment process.
2. The safety verification and validation activities, including the identification of the methodology and standards to be used throughout the development process.
3. The identification of the human factor issues that must be addressed by the design requirements.
4. The specific requirements for configuration management of all hardware, software, and documentation developed for the system.

3.1 Requirements and Concepts [49 C.F.R. § 236.905 (b) (1)]

The following requirements and concepts shall guide the development and implementation of safety-critical processor-based signal and train control systems on NS. Safety requirements for safety-critical processor-based signal and train control systems shall be established early in the system development process by performing a preliminary safety analysis, which results in a comprehensive list of all safety functions that the processor-based signal and train control system will perform. Safety requirements are intended to provide protection against potential unmitigated hazards associated with the implementation and operation of the safety-critical processor-based signal and train control system. The preliminary safety analysis shall utilize the methods and processes described below, which will regulate the quality assurance, design, development, testing, implementation, and maintenance of each product. The results of the preliminary safety analysis and the corresponding activities shall be documented in the Product Safety Plan (PSP).

3.1.1. Methods to Evaluate Behavior [49 C.F.R. § 236.905 (b) (1) (i)]

Appropriate hazard identification and evaluation techniques shall be used to evaluate total system behavior. Hazard analyses techniques that assess the risks associated with the potential system behavior hazards, as well as the design or procedural protections against those risks, are the preferred approach to this evaluation. Hazards will be identified by appropriate NS operations experienced line and staff personnel using the following methods:

- 1) Use intuitive “engineering sense”
- 2) Examine/inspect similar facilities and systems
- 3) Review performance expectations
- 4) Review codes, regulations and existing standards
- 5) Interview current or intended users or operators
- 6) Consult available hazard checklists
- 7) Review safety studies and analyses from other similar systems
- 8) Review historical documents: mishap files, near-miss reports, injury data, etc.
- 9) Consider external influences like weather and personnel tendencies
- 10) Consider all phases of implementation
- 11) Consider “common causes”
- 12) Brainstorm and consider “what-if?” scenarios

Acceptable hazard evaluation methodologies and techniques that may be used as a part of this process include the following:

- A. Preliminary Hazards Analysis (PHA)
- B. Functional Fault Tree (FFT) or equivalent
- C. Subsystem Hazard Analysis (SSHA)
- D. Operating & Support Hazard Analysis (O&SHA)
- E. Functional Hazard Assessment (FHA)

These hazard identification methodologies and the risk assessment procedures described in Section 3.1.2 shall be used to establish safety requirements to eliminate, mitigate, or control potential hazards. Appendix B to this RSPP provides additional information about NS recommended hazard evaluation methodologies and techniques.

3.1.2. Risk Assessment Procedures [49 C.F.R. § 236.905 (b) (1) (ii)]

A documented hazard risk assessment shall be performed that ranks each hazard in terms of severity and probability of occurrence. Once a hazard is identified, an analysis of its potential severity and probability of occurrence shall be performed. The process for this analysis shall be standardized¹. The following categories of probability and severity (taken from MIL-STD-882C) or an approved equivalent shall be used to perform the hazard risk assessment.

Hazard Severity is defined as a subjective measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, and/or procedural deficiencies for system, subsystem, or component failure or malfunction, and shall be categorized as follows:

- I. (Catastrophic) – Events that result in fatalities, multiple severe injuries, loss exceeding \$1,000,000, or irreversible severe environmental damage that violates law or regulation.
- II. (Critical) – Events that result in a single fatality, severe injury, loss greater than \$150,000 but less than \$1,000,000, or reversible severe environmental damage that violates law or regulation.
- III. (Marginal) – Events that result in minor injuries (FRA reportable), loss greater than \$10,000 but less than \$150,000, or mitigable environmental damage.
- IV. (Negligible) – Events that result in a single minor injury (FRA reportable), loss not exceeding \$10,000, or minimal environmental damage.

¹ While it is possible to develop a quantitative methodology for this type of analysis, the most practical method for railroad application is straightforward deductive reasoning, applied on a collective or organizational basis. A composite of experienced railroad personnel from appropriate line and staff departments can effectively determine the severity of all but the most difficult or unusual hazards.

Hazard Probability is defined as the probability that a specific hazard will occur during the planned life cycle of the system element, subsystem, or component. Hazard probability shall be ranked as follows:

A (Frequent) – Classification associated with a hazardous event that is likely to occur often in the life of the system, subsystem, or component, with a probability of occurrence greater than 10^{-2} per train hour.

B (Probable) – Classification associated with a hazardous event that will occur several times in the life of the system, subsystem, or component with a probability of occurrence less than 10^{-2} but greater than 10^{-4} per train hour.

C (Occasional) – Classification associated with a hazardous event that is likely to occur some time in the life of the system, subsystem, or component with a probability of occurrence less than 10^{-4} but greater than 10^{-6} per train hour.

D (Remote) – Classification associated with a hazardous event that is unlikely, but will possibly occur in the life of the system, subsystem, or component with a probability of occurrence less than 10^{-6} but greater than 10^{-8} per train hour.

E (Improbable) – Classification associated with a hazardous event that is so unlikely to occur that it can be assumed it will not be experienced in the life of the system, subsystem, or component with a probability of occurrence less than 10^{-8} per train hour².

Hazard Risk Assessment is the process of combining the hazard severity and hazard probability to determine which identified hazards are acceptable as is, acceptable with proper documentation, acceptable with sufficient mitigation, or unacceptable. A hazard risk assessment performed for NS shall use the following pre-approved matrix (Table 3.1) or an approved equivalent. The matrix shall be used to establish hazard risk, and set priorities for resolutions that eliminate, minimize, or control the hazards.

² The E (Improbable) category is not interpreted as zero probability, thus zero risk. The E (Improbable) category includes all items that are judged to have low or extremely low probability of occurrence. There is no zero probability category included in the ranking matrix.

Establishment of *safety requirements* shall result from formalized, predetermined procedures for hazard and risk resolution. *Hazard Resolution* is defined as the analysis and subsequent actions taken to reduce, to the lowest level practical, the risk associated with an identified hazard. Safety requirements shall be defined for hazards that present a risk that cannot be accepted because of severity and/or high probability (“unacceptable” risk index in Table 3.1) and thus must be eliminated by design or other explicit control measures.

<i>Table 3.1 Hazard Risk Resolution Matrix</i>				
Severity → Probability ↓	I. (Catastrophic)	II. (Critical)	III. (Marginal)	IV. (Negligible)
A (Frequent)	UN	UN	UN	AC
B (Probable)	UN	UN	UN	AC
C (Occasional)	UN	UN	AC/WR	AC
D (Remote)	UN	AC/WR	AC	AC
E (Improbable)	AC/WR	AC	AC	AC
<i>Codes</i>	<i>UN: Unacceptable</i> <i>AC/WR: Acceptable with review by NS management</i> <i>AC: Acceptable without review</i>			

Hazards with risk in the “acceptable with review” category shall be subject to appropriate hazard resolution procedures that eliminate, mitigate, or minimize the hazard risk to the satisfaction of NS³ with the approval of the Vice President of Operations, Planning and Support.

3.1.3. System Safety Precedence [49 C.F.R. § 236.905 (b)(1)(iii)]

NS requires that the Developer shall follow the order of precedence for satisfying safety-critical processor-based signal and train control system safety requirements and resolving identified hazards per this RSPP as follows:

1. Design for minimum risk. Eliminate hazards through design.
Minimize or eliminate the use of human input for safety-critical

³ Hazard resolution is not synonymous with hazard elimination. In a railroad environment, there are some hazards that are impossible to eliminate and others that are highly impractical to eliminate. Reduction of risk to the lowest practical level can be accomplished by applying appropriate safety design principles. Examples of these safety design principles are provided in MIL-STD-882C.

functions. Minimize or eliminate the use of data from external non-safety-critical systems for safety-critical functions. When human input, or data from external non-safety-critical systems is used for safety-critical functions, design to minimize or eliminate hazards from human input error, or from erroneous, out of sequence, or stale data from non-safety-critical systems. If an identified hazard cannot be eliminated, the associated risk will be reduced to an acceptable level through design selection and proper implementation using Safety Assurance Concepts (see Section 4.10 of this RSPP) to the satisfaction of NS with the final approval of The Vice President Operations, Planning and Support.

2. Incorporate safety devices. Reduce the hazard to an acceptable level through the use of fixed, automatic, or other protective safety design features or devices. Provisions shall be made for periodic functional checks and calibration of safety devices where applicable. Fail-safe devices may be provided as protection against hazards that can be caused by other system components.
3. Provide warning devices or labels. Use devices to detect potentially hazardous conditions and to produce adequate warning signals to alert personnel of the hazard. Warning signals and labels and their application shall assure a minimal probability of incorrect personnel reaction to the warning signals and shall be standardized within like types of systems. Warning devices and labels shall not be used where an alternative design could be reasonably engineered into a product whereby the alarm or label would not be required. All alarms and labels, not required by Law, are subject to the approval of NS.
4. Develop procedures and training. Procedures and training shall only be used with prior NS approval where it is impractical to eliminate hazards through design selection or to adequately reduce associated risk with safety and warning devices. Procedures may include the use of personal protective equipment.

3.1.4. Safety Assessment Process Requirements [49 C.F.R. § 236.905 (b)(1)(iv)]

Safety-critical processor-based signal and train control systems placed in-service on NS shall be implemented and managed using a comprehensive safety assessment process that addresses safety concerns for the life cycle of the system. This safety assessment process shall be focused on identifying and resolving hazards associated with the system. The developer and NS shall execute and document this process as part of the

PSP where appropriate. The framework of this safety assessment process focuses on the following elements:

- 1) Identifying potential hazards that may occur throughout the system life cycle (through living records as specified in Section 3.1.1 and Appendix B of this RSPP).
- 2) Understanding the impact on safety of the potential hazards by quantifying the risk associated with each hazard (through living records as specified in Section 3.1.1 and Appendix B of this RSPP).
- 3) Establishing hazard-tracking mechanisms to ensure that resolution measures (i.e., system safety requirements, rules, processes, and procedures are taken as appropriate to eliminate, minimize, or control unacceptable hazards. Such tracking mechanisms are subject to version history and a hazard coding/logging system that tracks any particular hazard horizontally to mitigation within its own system or subsystem and vertically to indicate any effects to other systems and/or subsystems. Such records shall indicate the related system, subsystem, unique hazard numbered designation, target (affected entity, such as personnel, equipment, downtime, product, environment, etc), probability, severity, proposed mitigation, and state of the hazard following mitigation.
- 4) Performing safety verification and validation to demonstrate system safety.
- 5) Monitoring testing and system operations to ensure achievement of safety requirements.
- 6) Evaluating the impact of specification changes, software problem reports and engineering change notices.

The Safety Assessment Process (SAP) shall consist of three categories of work. A qualitative effort that logically compiles the hazards and mitigations that are identified through the processes described in Section 3.1.1 and Appendix B. The qualitative review should be comprehensive and shall endeavor to discover voids in coverage for any known hazard and any hazards that may have been overlooked. There will be a quantitative analysis wherein known or estimated values are used to assess system safety in a numerical sense, using values such as Mean Time to Hazardous Event (MTTHE), Mean Time to Failure (MTTF) or other documented measurement techniques. This process shall also include a comparison to the existing system and method of operation in accordance with the minimum requirements stated in § 236.907. The SAP shall consider and use historical hazard and mishap data, including lessons learned from other systems. The SAP shall demonstrate that all risks have been eliminated or mitigated to the lowest practical level, and

shall be used to monitor and confirm the safety performance of the system through its life cycle. The safety objectives shall be compared to the current performances to confirm that they continue to be achieved by the system. The Developer's use of an alternative safety assessment methodology must be approved by NS and be acceptable under the requirements of § 236.

3.2 Design for Verification and Validation (V&V) [49 C.F.R. § 236.905 (b) (2)]

Safety-critical processor-based signal and train control system development and implementation process shall include safety verification and validation. System safety verification and validation (V&V) comprises a set of safety activities for a system based on a set of analyses, tests, simulations and calculations that together establish the technical evidence necessary to demonstrate compliance with all applicable safety requirements.

Safety validation activities shall demonstrate that the correct system is built. Safety validation involves those activities that demonstrate the overall integrated system, and each portion thereof, performs the correct safety functions.

Safety verification activities shall demonstrate that the system is built correctly, and include those activities that demonstrate the system has been designed and implemented with the required level of safety from a qualitative and quantitative standpoint, including showing that all unacceptable hazards have been mitigated or eliminated.

To minimize the extent of safety V&V required to satisfy the requirements of this RSPP, safety-critical functions shall be designed so they are isolated or partitioned to operate as independently as possible from the other non-safety-related functions.

3.2.1. Methodology

Appendix C to this RSPP provides the NS recommended methodology for safety verification and validation activities.

3.2.2. Standards

The safety V&V activities shall incorporate requirements and guidance from existing and evolving standards for safety V&V of hardware and software in safety critical railroad systems. Applicable standards shall be identified in the PSP and adhered to throughout the safety V&V process to demonstrate that best available consensus practices have been followed

to demonstrate safety of the processor-based signal and train control system. The PSP shall clearly identify individual standards and requirements that will be used in the design, development, installation, and testing of the product. 49 C.F.R. Part 236, Appendix C defines appropriate and acceptable standards for use in developing the PSP and the V&V process for a given processor-based signal and train control program. Non-published standards shall only be used with prior NS approval.

3.2.3. Documentation

All safety V&V activities shall be sufficiently documented to record the specific activities undertaken and their results. This documentation shall provide a credible audit trail for project team review and/or a possible independent, third party review and assessment that the safety V&V activities were comprehensive and adhered to best practices.

Documentation of V&V activities shall include the following requirements:

- Traceability links between all relevant design and safety program documents. This includes linking of identified hazards to their specific mitigation at each level of the requirements, design, operational instructions/warnings, and test documentation.
- Description of the safety V&V methodologies employed.
- Identification of standards, processes, and other reference documentation (e.g. design documents).
- Testing methodology, procedures, and test results.
- Description of the specific safety requirement(s) examined in each V&V activity.
- Discussion of qualitative and/or quantitative conclusions resulting from the V&V activity.
- Cross references to previous hazard analyses, the hazard log, hazard resolution actions, evidence that hazards were resolved (controlled, mitigated or eliminated), and the safety V&V activity that demonstrated compliance with safety requirements.

3.2.4. Independent Review and Assessment of Verification and Validation

When required, an independent review and assessment of the product safety verification and validation activities shall meet the requirements set forth in 49 C.F.R. Part 236, Appendix D and NS departmental product specific standards and procedures.

3.3 Design for Human Factors [49 C.F.R. § 236.905 (b)(3)]

The PSP shall contain a human factor analysis, which shall include a complete description of all of the human machine interfaces and the safety functions performed by humans while the system is in operation. The PSP shall identify human factor issues, including those set forth in 49 C.F.R. Part 236, Appendix E and shall document the manner in which the design of the safety-critical processor-based signal and train control system addresses each human factor issue identified.

The HMI analysis shall consider systems and practices already in operation on NS. HMI analysis should specifically determine the effect of any proposed changes in operation and the benefit versus degree of change difficulty. While it is understood that the human factors requirements of a system shall be compliant with NS operating rules, special instructions, procedures for safe operation and any applicable Federal regulations, there may be compelling reason (for improved safety or other operational benefit) to propose a change in rule or operation. In such case, recommendation will be made by the Developer for approval by the Vice President Operations, Planning and Support. Should such recommendation be accepted and prior to any operational changes, appropriate NS representative(s) will follow existing procedure(s) to enact such a change.

3.4 Configuration Management Control Plan [49 C.F.R. § 236.905(b) (4)]

Formal methods for configuration control and associated documentation shall accompany design and development of a safety-critical processor-based signal and train control system. This documentation shall clearly identify those control measures that manage system safety functional requirements and hazard resolution actions for a system. Such identification shall be provided in documents and databases using a consistent symbol, word or unique character that means "safety-critical".

A Configuration Management Plan (CM) establishes the CM practices to be used on all hardware, software and documentation developed for NS in safety-critical processor-based signal and train control systems under this Subpart H. The Developer shall be responsible for ensuring the plan utilizes existing change control procedures that are consistent and compliant with the safety levels established with the new system. NS will review and approve the Developer's proposed CM to ensure that it is compliant with NS requirements so it can be integrated into defined processes. Any recommendation not compliant with NS' CM shall be reviewed by NS and either 1) rejected in which case the Developer shall modify its recommendation while maintaining the safety of the system or 2)

accepted in which case such changes in NS' CM shall be documented, approved and integrated in accordance with existing practices and procedures.

The Configuration Management Control Plan and its associated processes shall, at a minimum:

1. Identify the process and procedures that are required to be compliant with the CM including the defined method to modify or change such processes and/or procedures.
2. Require a living database of covered equipment including:
 - a. Name of equipment, including version, model and other appropriate forms of identification.
 - b. Name and description of subcomponents, including version, model and other appropriate forms of identification.
 - c. Location.
 - d. Software and hardware identification features including current version, model, etc for each particular location.
 - e. Revision and/or modification history.
 - f. Identification of any predefined changes, revisions, modifications and/or capabilities that may not be utilized in the existing operation but exist within system or component capabilities. (In the case of system features, these may be discussed in the PSP [49 C.F.R. § 236.907] as features included but not utilized. Those system features will not be included in the CM).
3. Provide for secure access by end users.
4. Provide protection against unauthorized access and modification.
5. Provide for a historical record of changes, revisions, etc including unique identification of users and /or those authorized to make modifications.
6. Where components listed in the CM database are involved, provide for traceability and tracking for hazards not previously identified [See Monitoring of Operational Service 49 C.F.R. §§ 236.917 (b) and 236.907 (a)(18)]

3.5 Railroad Safety Program Plan Modifications [§ 236.905(d)]

NS may find the need to modify its RSPP. Modifications to the finalized and FRA approved RSPP will need to be requested and approved through the Office of the Vice President of Operations, Planning and Support on NS. Any RSPP modifications related to safety-critical PSP requirements will require additional approval from the FRA.

4. Product Safety Plan (PSP) [49 C.F.R. § 236.907]

The Developer shall prepare, with the assistance and final concurrence of NS, a Product Safety Plan that is compliant with this RSPP and all applicable FRA regulations for the equipment included in the safety-critical processor-based signal and train control system. The PSP shall describe the product in detail, both physically and operationally. The PSP shall include acceptable criteria for the development, installation, implementation, operation, maintenance, repair, inspection, testing and modification of the product.

The minimum requirements described below include various analyses, test results, and other documentation that support the Developer's safety program and activities. This documentary evidence may be incorporated in the PSP in its entirety, or prepared as separate documents and appropriately referenced in the body of the PSP. All documentary evidence supporting the PSP shall be available for review and audit by NS and/or NS's designee.

The PSP must include:

A complete description of the methods used to evaluate a system's behavioral characteristics.

- A complete description of the risk assessment procedures.
- A statement indicating the system safety precedence followed and that such precedence meets the requirements of this RSPP.
- Identification of the safety assessment process.

4.1 Description of the Product [49 C.F.R. § 236.907 (a)(1)]

The PSP shall contain a complete description of the product, including a list of all components and their physical and functional relationship, which meets the following minimum requirements:

- A description of the role of the product in the overall train control system operation, including interfaces and interactions with existing systems and/or equipment.
- Identification of any subsystems and/or modules that make up the product, including their function within the overall product.
- Evidence that the product as designed, manufactured, tested, and assembled will meet the system safety requirements as established by NS and applicable FRA regulation.

The following shall be provided as acceptable evidence:

1. A description of the Developer's system design practices
2. A System Management Plan that shall include:
 - a. Software Management Plan
 - b. Quality Assurance Management Plan
 - c. Test Management Plan
 - d. Verification and Validation Management Plan
 - e. Problem Management Plan that covers both Software and Hardware
3. A description of the Developer's software and hardware development practices with respect to industry best practices, including compliance with generally accepted standards
4. A description of the Developer's quality control and problem management processes.

4.2 Description of Railroad Operations [49 C.F.R. § 236.907 (a)(2)]

The PSP shall describe the railroad operation or categories of operations for which the product is designed to be used. This description shall include the relevant NS physical infrastructure and current and planned operations. The description shall include train volume, load volume, passenger train volume, joint operations, hazardous material volume, NS operating rules, special instructions, operating speeds, and other physical and operating characteristics to completely describe the operating environment. The PSP shall also describe the maximum train volume, train frequency, operating speed, and other physical capacities as applicable, for which the system is designed.

4.3 Operational Concepts Document [49 C.F.R. § 236.907 (a)(3)]

The PSP shall describe the product's operational concepts, the functionality of the various subsystems and/or modules, and information flows within the system. This description shall include the product's operational concepts as defined for both normal and abnormal operating conditions.

4.4 Safety Requirements Document [49 C.F.R. § 236.907 (a)(4)]

The PSP shall identify the initial and derived requirements necessary for the safe operation of the product for its intended application. These safety requirements shall be established through use of accepted analysis techniques and shall include both hardware and software safety requirements as necessary. Each safety requirement shall be further defined by the specific functions that must be implemented in a particular subsystem or component of the product in order to satisfy the given safety requirement.

4.5 Product Architecture Document [49 C.F.R. § 236.907 (a)(5)]

The PSP shall describe the product architecture and how it satisfies each safety requirement at the overall system level. These System Safety Concepts shall be identified as part of the overall architecture of the system in order to support safe operations. The documentation shall describe both hardware and software aspects of the product architecture and shall identify the protection developed against random hardware faults and systematic errors. The documentation shall also identify the extent to which the architecture is fault tolerant.

4.6 Hazard Log [49 C.F.R. § 236.907 (a)(6)]

A Hazard Log provides a specific description of the hazards that must be addressed throughout the life cycle of the product, as derived from the product functionality, operating methods, and the hazard analysis. The PSP shall include a formal Hazard Log and describe the methods used for tracking the identified hazards to ensure that these hazards are resolved in the system design.

Each hazard description shall include a stated threshold level (residual hazard risk index) that, if exceeded, would be unacceptable. In addition, any hazard with a hazard severity ranking of I or II (potential for death, system loss, or serious injury) shall be designated as a Safety Critical Item and clearly identified as such in the Hazard Log. Safety Critical Items shall require completion of the defined resolution action prior to system operation. The Hazard Log shall be updated throughout the product or system development as actions are completed to resolve the hazards identified.

The Hazard Log shall contain the following information for each identified hazard and safety-critical item:

- A unique hazard identification number.
- Description of the hazard.
- References to the safety program or development activity where the hazard was identified and source document traceability supporting the hazard identification.

- Risk ranking of the hazard.
- Proposed resolution for the hazard.
- Assignment of responsibility for the resolution action to a program function/organization.
- Status of the hazard resolution action, including actions taken, date of actions, review and approval of the action, and references to source documents supporting the action.
- Notation of whether the hazard is OPEN (requiring further action) or CLOSED (resolution action(s) complete and approved by NS).
- A description of the organizational structure established by the Developer that insures independence and integrity of the safety process.

4.7 Risk Assessment Requirements [49 C.F.R. § 236.907 (a) (7)]

The PSP shall include a risk assessment of identified hazards consistent with the risk assessment strategy defined in Section 3.1.2 of this RSPP, 49 C.F.R. § 236.909, and 49 C.F.R. Part 236, Appendix B. The risk assessment shall include system hardware, software, human elements, and their interfaces and shall address both hazard severity and probability of occurrence. Hazards that are identified as having an unacceptable or undesirable risk shall be eliminated by design or mitigated such that the risk is acceptable or can be controlled through the appropriate application of existing operating rules, operating practices and/or procedures. These hazards shall not be mitigated by the imposition of new operating rules, operating practices, and/or procedures without prior approval of NS in accordance with this RSPP. The risk assessment shall clearly identify the risks that require mitigation, the mitigation strategy employed, and justification for the determining the reduced risk level. Alternatively, an abbreviated risk assessment may be developed per Section 6.2.2 of this RSPP and 49 C.F.R. § 236.909 (d), if the system introduces no new hazards and the MTTHE is equal to or greater than that of the system it is replacing.

If a proposed system is interfaced with systems or components that are external (not an integral part of) the proposed system, a Subsystem and/or Interface Hazard Analysis and Hazard Mitigation Plan shall be included in the PSP.

4.8 Hazard Mitigation Analysis [49 C.F.R. § 236.907 (a) (8)]

The PSP shall document the process employed to identify potential hazards associated with the product and the safeguards employed to eliminate, mitigate, or control the hazards in the product design. The Developer shall describe any operation or maintenance-related safety requirements that are necessary to safely deploy the product on NS.

Appendix B to this RSPP provides the NS recommended direction for hazard identification and mitigation techniques that may be used by the Developer in complying with these requirements.

4.9 Safety Assessment and V&V Process [49 C.F.R. § 236.907 (a) (9)]

The PSP shall describe the safety assessment and V&V process conducted during product development and shall define the V&V process necessary to safely deploy the product. The PSP shall describe how the safety assurance criteria and processes covered in 49 C.F.R. Part 236, Appendix C are addressed directly or indirectly through other safety criteria, or are not applicable. The V&V process shall include all or part of the following activities, as appropriate:

- Process audits and/or analyses.
- Verification tests of product and/or module functions.
- Factory and/or manufacturing tests.
- Qualification testing to validate adequacy for specific applications.
- Systems integration tests.
- Field acceptance/commissioning/operational tests.
- Documentation of traceability of hazards to specific mitigation at each level of requirements, design, operation instructions/warnings, and test.

Each V&V activity shall be fully documented throughout the V&V process and available to NS or the NS designee for audit of the V&V activities.

Appendix C to this RSPP provides the NS recommended direction for safety verification and validation activities that may be used by the Developer in complying with these requirements. The FRA may require an independent third party assessment of the product V&V process based on the factors described in the 49 C.F.R. § 236.913 (h). The requirements for this assessment are covered in 49 C.F.R. Part 236, Appendix D.

4.10 Safety Assurance Concepts [49 C.F.R. § 236.907 (a) (10)]

Safety Assurance Concepts used to ensure the operational safety of any safety-critical functions that are implemented in the product being developed shall include in the PSP a complete description of the safety assurance concepts used including and explanation of the design principles and assumptions PSP shall include a description of the specific Safety Assurance Concepts that are used to implement the hardware and software in a safe manner at a subsystem or function level. The underlying design principles and application assumptions for the Safety Assurance Concepts being used shall be identified, along with appropriate verification methods that will show that the Safety Assurance

Concepts are correctly and completely implemented in the product design. The Safety Assurance Concepts shall each be described with regard to the following characteristics:

- a) The fundamental premise;
- b) Specific assumptions as to the operating environment;
- c) Certain dependencies on completeness of concept application, and;
- d) Specific methods that are used to verify that the concept has been adequately applied.

The description of the Safety Assurance Concept(s) used in the safety critical processor based signal or train control system shall each be described with regard to the above listed characteristics.

4.11 Human Factors Analysis [49 C.F.R. § 236.907 (a) (11)]

The PSP shall include a human factors analysis that identifies human machine interfaces that are important to safe operation and maintenance of the subject system. The analysis shall describe the type of human action or function that is required to ensure safety, describe the designed features of the equipment to facilitate human interaction with the equipment, and provide justification of how these design features reduce the potential for human error during operation and maintenance of the equipment.

The human factors analysis shall include a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the subject system to enhance or preserve safety, and an analysis describing how human factors that are covered in Appendix E to part 236 are addressed directly, addressed using other criteria or are not applicable.

The scope and techniques of the human factors analysis shall be adequate to show that the product or system complies with all of the applicable requirements in 49 C.F.R. Part 236, Appendix E or equivalent criteria that have been established as acceptable to the FRA.

4.12 Training Requirements [49 C.F.R. § 236.907 (a) (12)]

The Developer shall define in the PSP, the training requirements necessary for NS personnel to ensure safe operation of the product. These training requirements shall address installation, normal and abnormal operation, repair, maintenance, modification, and testing of the product. The PSP shall identify the intended audience for each training requirement. The Developer and NS shall jointly develop all training requirements.

4.13 Test Procedures and Equipment [49 C.F.R. § 236.907 (a) (13)]

The PSP shall document test procedures and identify requirements for test equipment (as needed) for the maintenance of the product to ensure the safe operation, installation, repair, modification and testing of the product. The test procedure documentation shall include specific safety test procedures, test equipment requirements, description of acceptable safety test results, and appropriate repair, replacement, and/or modification actions required when test results are deemed unacceptable. The procedures, including any calibration requirements, shall be consistent with system needs, and shall contain an explanation of any deviation from the recommendations of the Developer of the equipment. The following types of testing activity shall be included under this requirement:

- Qualification testing designed to demonstrate that the product is suitable for a particular application, performed at the factory, on a test track, or on an operating line of the railroad.
- Scalability testing designed to demonstrate that the system is fully integrated and stress tested.
- Implementation testing designed to ensure that the product has been installed correctly, and is operating safely and functioning as intended.
- Operational testing designed to ensure that the product is operating safely and functioning as intended after the product has been modified or disarranged, or after maintenance has been performed.
- Periodic testing to ensure that the product continues to operate safely and function as intended.

Test procedures shall address the testing frequency necessary to demonstrate that safety requirements, safety critical hazard mitigation processes, and safety critical tolerances are not compromised over time, through use, or after maintenance is performed.

4.14 Applicability to Other Rules and Regulations [49 C.F.R. 236.907 (a) (14)]

The PSP shall list the rules and regulations of the requirements of Part 236 Subparts A – G that do not apply or are satisfied by the product using an alternate method as required 49 C.F.R. §§ 234.275 (c) or 236.901 (c)(1). Each citation of a rule or regulation shall be accompanied by a justification of why the rule or regulation does not apply or how the product satisfies the rule or regulation.

4.15 Security Measures for the Product [49 C.F.R. § 236.907 (a) (15)]

The PSP shall describe security measures for the protection of the product. The security measures shall address train-borne, wayside, and centrally located train control subsystems and/or components as applicable. Security measures shall be designed to limit unauthorized access to and prevent tampering or overriding the safety functions of the product. Specific security measures shall be designed to prevent unauthorized access to and/or spoofing of safety-critical messages wherever these messages are communicated via radio, internet or public switched network.

4.16 Warnings and Warning Labels [49 C.F.R. § 236.907 (a) (16)]

A complete description all warnings shall be placed in the Operations and Maintenance Manual as required by 49 C.F.R. § 236.919 and Section 8 of this RSPP. The description shall also include all warning labels placed on system equipment as necessary to ensure safety. These warnings shall address hazards to personnel safety and operational safety when inspecting, testing, or maintaining the train control equipment.

As noted in the System Safety Precedence called for in Section 3.1.3 of this RSPP, warnings and labels shall be used when other mitigation methods do not eliminate the hazard from affecting system user interfaces. The use of warnings and labels shall not be the primary mitigation for hazards with catastrophic severity. Warnings and labels shall be noted and explained during training for users of the system and/or its subsystems.

4.17 Implementation Testing [49 C.F.R. § 236.907 (a) (17)]

The PSP shall contain descriptions of the pre-implementation (factory) and implementation (field) testing procedures that will demonstrate that the safety critical requirements are met and the safety critical hazards are mitigated to the appropriate level.

Pre-implementation (factory) testing shall be shown to verify (by requirement and/or hazard tracing) the mitigation of all identified hazards by the system as developed, the proper use of Safety Assurance Concepts, the implementation of all safety-critical subsystem design requirements, and to validate that the system operates in a safe manner per the overall system requirements and architectural safety concepts.

Implementation (field) test procedures shall comprehensively establish that all safety-critical and functional requirements are met and that safety-critical hazards

are appropriately mitigated by the system as installed on the railroad. These detailed field test procedures shall include measures to provide for the safety of train operations during field test and cutover.

The Developer shall provide NS with the test plans and procedures developed per this requirement, and obtain approval of test plans and procedures from NS, prior to any testing.

4.18 Post Implementation Testing and Monitoring Procedures [49 C.F.R. § 236.907 (a) (18)]

The PSP shall describe the procedures, including time intervals, for maintaining safety critical subsystems once they have been installed and implemented in the field. Post-implementation or operational testing and monitoring procedures shall be created by the Developer and shall demonstrate that the equipment is functioning as intended, that system performance is not degraded over time, and that safety requirements continue to be satisfied. In addition, post-maintenance testing procedures shall be created by the Developer to demonstrate that the equipment has been restored to safe operating condition after performing maintenance activity (repair, replacement, and/or adjustment).

The PSP shall describe each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments and the system's resulting condition, including records of component failures resulting in safety-relevant hazards as required by 49 C.F.R. § 236.917 (b)(3).

The Developer shall provide NS with the test plans and procedures developed per this requirement. NS will approve test procedures prior to implementation and will insure testing and monitoring are executed.

4.19 Safety-Critical Assumptions [49 C.F.R. § 236.907 (a) (19)]

The PSP shall describe the assumptions made in the Developer's system architecture to ensure that the system meets NS requirements for availability without compromising the safety-critical requirements that also apply to the operation. Such descriptions shall include, for example, all backup methods for continued safe operation in case of system or sub-system failure. The description of the failure scenario assumptions shall be specific to each unique subsystem or component of the system design.

4.20 Incremental and Predefined Changes [49 C.F.R. § 236.907 (a) (20)]

If applicable, the PSP shall provide a detailed description of any pre-defined changes that may be made after initial implementation and how those changes are included in the other parts of this PSP to preclude having to file an amendment to the PSP. This documentation shall describe how these changes satisfy the minimum performance standard (as good as or better than the system it replaces), and do not compromise the system's safety-critical requirements for hazard mitigation. In addition, this section of the PSP shall define how any changes that involve slightly different specifications are verified and validated for safety-critical functions.

4.21 Communication of Hazards [§ 236.907(d)]

The PSP shall specify all contractual agreements with hardware and software external product suppliers for immediate notification of any and all safety-critical software upgrades, patches, or revisions for their safety-critical processor-based signal or train control system, subsystem, or component. Also included in this notification shall be the reasons for such a change and any interim remediation for an identified hazard that can affect the intended purpose of the system. These notifications shall be required whether or not the NS has experienced a failure of the system.

The PSP shall specify the NS's procedures for action upon notification of a safety-critical upgrade, patch, or revision for the processor-based system, subsystem, or component, and until the upgrade, patch or revision has been installed. These procedures shall be consistent with the criterion set for in § 236.915(d) as if the failure had occurred on NS.

The PSP shall identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change. The configuration/revision control measures must also include methodologies that allow these changes to be audited.

5. Minimum Performance Standard [49 C.F.R. § 236.909]

5.1 Performance Standard for Safety Risk Management [§ 236.909(a) and (b)]

The safety analysis included in the PSP will establish, with a high degree of confidence that the implementation of the subject safety-critical processor-based signal or train control system, subsystem, or product not result in risk that exceeds the previous condition. NS will make sure that the standard is met and will make available to the FRA the necessary analyses and documentation.

5.2 Performance Standard for Safety Risk Measurement [§ 236.909(a) and (b)]

The safety analysis must establish with a high degree of confidence that the introduction of the safety-critical processor-based signal or train control system will not result in a risk that exceeds the existing level of operation. A common risk metric shall be used to allow comparison of the safety performance of the existing and the new system under the operating scenario. Faults and failures that must be considered include hardware failures, software errors, human errors, and external influences. FRA will have access to the necessary NS analyses and documentation.

Section 236.913(g) (2) documents the railroad's PSP requirements for preparation, and FRA notification.

5.3 Risk Assessment Scope [§ 236.909(c) and (d)]

Section 236.909(c) and (d) identifies the proposed standards for the scope of the risk assessment to be conducted.

1. Abbreviated risk assessment: An abbreviated risk assessment demonstrates that the resulting MTTE for the safety-critical processor-based signal or train control system is greater than the MTTE for the existing method of operation. This determination must be supported by a credible safety analysis and concurrence from NS that an abbreviated risk assessment is acceptable. Use of AREMA standard development is authorized for abbreviated risk assessment on a case-by-case basis as designated by the NS and where appropriate.

An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard. The abbreviated risk assessment must show compliance with the performance standard by:

- a) Indicating that no new hazards are introduced as a result of the safety-critical processor-based signal or train control system;
 - b) Demonstrating that the severity of each hazard associated with the previous existing method of operation condition does not increase;
 - c) Demonstrating that the exposure to such hazards does not change from the previous existing method of operation condition.
2. Full risk assessment: A full risk assessment must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This includes risks associated with the previous condition, which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature (probability of occurrence or severity) is nonetheless affected by the change. A full risk assessment includes both qualitative and quantitative measures.
- a) Safety levels must be measured using competent risk assessment methods and must be expressed as the total residual risk in the system over its expected life-cycle after implementation of all mitigating measures. Appendix B to Part 236 – Risk Assessment Criteria, provides criteria for acceptable risk assessment methods. Other methods that are accepted standards and practice may be used.
 - b) The risk level must be adjusted for exposure for the previous condition. Exposure must be expressed as total train miles traveled per year. Severity must identify the total cost, including fatalities, injuries, property damage, and other incidental costs.
 - c) Planned changes in the physical and operating conditions that are coincident with the introduction of the new processor-based product require the adjustment of the previous condition to reflect any associated impact on risk. An example would be the adjustment of the previous system to support higher train speeds or densities.

5.4 Risk Assessment General Principles [§ 236.909(e) (2) and (3)]

The acceptable methods and the general principles for conducting risk assessments are documented in § 236.909(e) (2) and (3). Three variables must be provided with risk calculations: accident frequency, severity, and exposure. Any concurrent changes in railroad operations such as increased

train volumes, passenger volumes, and/or operating speeds resulting from the implementation of the safety-critical processor-based signal or train control system must be analyzed for the total change in risk, and then separately to identify and distinguish risk changes associated with the use of the system from risk changes due to changes in operating practices (increased operating speeds, etc.)

5.5 Monitoring of Operational Service [49 C.F.R. §§ 236.917 (b) 236.907 (a)]

NS will monitor actual system performance after the processor-based signal and train control system is placed in operational service. The monitoring program shall maintain a database of safety-relevant hazards and monitor their occurrence rate, even if no incidents or mishaps occur due to the hazard. Hazards whose occurrence rates are observed to exceed the specified occurrence rate (i.e., have a smaller observed MTTE or other measure than was stated in the PSP for the mitigating function) shall be reported to the FRA and additionally mitigated as required by 49 C.F.R. § 236.917 (b) (2).

This process shall encompass the requirement for monitoring of the system risks that relate to ongoing operation and maintenance. The Developer shall comply with both Section 4.18 of this RSPP and with 49 C.F.R. § 236.907 (a)(18) in this regard. The Developer, in co-ordination with NS, will provide for the life cycle of the product adequate documentation to demonstrate that the PSP meets the safety requirements of NS's RSPP and applicable standards in this subpart including the risk assessment. The Developer shall promptly notify NS if the risk assessment has been negatively affected by the field experience.

The NS monitoring program will also identify the occurrence of hazards associated with the product that were not previously identified in the PSP. Hazards that were not previously identified in the PSP shall be assumed to have a threshold level MTTE of zero and shall be subject to the requirements of 49 C.F.R. §§ 236.917 (b) (2) and 236.907 (a) (6)].

6. PSP Review and Approval [49 C.F.R. §236.913]

6.1 Railroad Review and Approval of PSP [49 C.F.R. § 236.913 (c) - (e)]

All PSP's developed or amended for the implementation and operation of products on NS shall be reviewed and approved by NS before submission to the FRA. The suitability and readiness for submission of any PSP, or PSP revision, to the FRA by NS shall be the sole discretion of NS.

7. Implementation and Operation [49 C.F.R. § 236.915]

7.1 Compliance with PSP and RSPP Requirements [49 C.F.R. § 236.915 (a), (b)]

Implementation of a safety-critical processor-based signal and train control system shall be in compliance with all requirements within this RSPP, the approved PSP, and 49 C.F.R. § 236.915 (a) prior to beginning operations. Evidence of compliance shall be established through review of documentary evidence, safety V&V testing, or other reviews or analyses necessary to establish compliance with safety requirements. Evidence of compliance shall be documented.

Railroad operations after implementation of the product shall remain in compliance with the operational design limits as specified in the PSP as required by 49 C.F.R. § 236.915 (b).

7.2 Restrictions on Testing [49 C.F.R. § 236.915 (c)]

NS shall establish and document procedures to ensure safe train movement and operations during testing of safety-critical processor-based signal and train control system modules, systems, or subsystems. These procedures shall be specific to the product being tested and shall be integrated into standard testing and maintenance procedures and training programs for test and maintenance personnel.

7.3 System or Subsystem Failures [49 C.F.R. § 236.915 (d)]

The failure of safety-critical processor-based signal and train control systems, subsystems, or components to perform as intended shall be adjusted, repaired, or replaced without undue delay. Failures shall be investigated by the NS department that is responsible for the maintenance of the product, to determine cause and where necessary, resolution action taken to prevent or reduce the probability of recurrent failure. Safety of train movements and of roadway workers must be ensured during the adjustment, repair, or replacement process.

8. Operations and Maintenance Manual [49 C.F.R. § 236.919]

A combined Operations and Maintenance Manual, herein after referred to as the OMM, shall be delivered to NS by the Developer in an agreed upon manner. The OMM shall be based on the system specific procedures specified in the PSP and consistent with NS overall operating rules and special instructions as well as applicable department specific standards and procedures. The manual shall address the installation, maintenance, repair, modification, inspection, testing, and operations under normal and failure modes associated with the product. Responsible Departments will ensure that all employees identified by this PSP will have access to the section(s) of the OMM that applies to their respective area of responsibility to properly perform such tasks. NS shall properly catalog the contents of all sections to create a Master OMM. The Master OMM will be available for inspection by the FRA and/or FRA approved designees in the library created for the product at the NS Headquarters in Atlanta Georgia. Applicable sections will be available for inspection by the FRA and/or FRA approved designee(s) at field sites where such products are deployed or maintained. Additionally, legible current and corrected plans required for the proper installation, maintenance, repair, modification, inspection, and testing of the system shall be delivered by the Developer or a third party supplier, and copies maintained by NS where such products are deployed or maintained. The plans shall provide sufficient detail, including the identification of all software versions, revisions, and revision dates.

The NS Configuration Management Control Plan identifies the control measures needed to ensure that the current hardware, software, and firmware revisions are documented and included in the OMM and plans where relevant. The Developer shall comply with the requirements in this plan, as well as any additional configuration/revision control measures specified in the PSP.

All safety-critical components shall be positively identified, handled, replaced, and repaired per specific procedures described by the Developer in the OMM as part of the PSP. Such procedures must meet the product specific requirements of NS existing operating rules and special instructions rules as well as specific departmental standards and procedures that apply to the product. These rules and procedures will be provided to the Developer by NS for inclusion in the OMM. Applicable NS rule books and procedure manuals referenced in the PSP and OMM for a specific product will be retained in a library at the Atlanta Headquarters of NS. Such procedures shall be designed to preserve the safety characteristics of the product and components.

9. Training and Qualification Program [49 C.F.R. §§ 236.921 - 236.929]

NS will establish and implement training and qualification in conjunction with the requirements of the developer's specifications listed in the RSPP. NS will coordinate with the developer to create training and qualification based on product specific requirements, NS operating rules, special instructions and departmental specific standards and procedures covered in the PSP. All training must be approved by NS prior to implementation.

Training and qualification programs for persons whose duties require interaction with the safety-critical processor-based signal and train control systems will be coordinated with each responsible NS department for establishment and implementation. These programs will address the minimum NS training and qualification requirements, as well as those described in the PSP, for workers whose duties include:

- Issuing or communicating mandatory directives in territory where a processor-based signal and train control system will be used;
- Operating trains or serving as a train crew member in processor-based signal and train control system territory;
- Installing, inspecting, testing, maintaining, modifying, or repairing safety-critical processor-based signal and train control systems, subsystems, or components, including central office, wayside, or onboard equipment, and;
- Roadway workers whose duties require them to know and understand how a train control system affects their safety and how to avoid interfering with its proper functioning;
- Direct supervisors of designated employees covered in this PSP.

NS training programs will address both initial training and continuing training programs necessary to maintain worker knowledge skills. Prior to the completion of a required training program, persons whose duties require them to perform tasks associated with a processor-based signal and train control system may perform such tasks under the direct on-site supervision of a qualified person. Training program design, execution, and record keeping shall be in accordance with the requirements specified in the 49 C.F.R. §§ 236.921, 236.923, 236.925, 236.927, and 236.929, as well as those in applicable parts of Title 49 of the Code of Federal Regulations.

10. Human-Machine Interface [49 C.F.R. Part 236, Appendix E]

NS recognizes that safety-critical processor-based signal and train control systems may entail human interaction with potentially complex functions that provide safety to the railroad. NS therefore requires that the Developer use ergonomic design criteria as specified in the development of the Human Machine Interface (HMI). The Developer shall describe the proposed HMI features of the system for NS approval as part of the design documentation. Proper reference to the specific design documents shall be included in the PSP for completeness.

Proper design of HMI will support vigilant attention by the operating personnel and encourage appropriate action where needed to ensure safety of the railroad operation. HMI designers must be familiar with the processor-based train control system and its operating environment. Railroad personnel knowledgeable in the operation of the system shall be included in any HMI design. The following shall be considered as requirements for the HMI of the Developer's system:

1. The system shall require regular operator interactions or shall alert the operator.
2. The system shall provide timely feedback in response to operator inputs or changing conditions, with an understandable explanation of the content of the feedback.
3. The system shall prompt operators for necessary input in advance of the time the input is needed.
4. The HMI shall provide consistent and predictable display of information and use consistent formats for obtaining necessary inputs from the operator.
5. The system shall arrange and integrate information to facilitate the operator's ability to respond correctly.
6. The system design shall use simple standardized formats that minimize time to respond to information presented.
7. The system shall provide automatically refreshable display that can supplement the operator's memory.
8. The system design shall optimize the location, size, color, and movement of HMI controls used by the operator.

-
9. The system shall consider data importance and operator conspicuity in developing HMI display of safety-critical information.

The Developer shall perform design trade-off tests using typical personnel or cite existing NS standards to demonstrate to the satisfaction of NS that the effectiveness of the HMI has been optimized for the purposes of the system. The Developer approach to the items 1-9 above shall be documented in the PSP.

For further guidance, NS refers the Developer to FRA regulations in 49 C.F.R. Part 236, Appendix E.

11. APPENDIX A – Applicable Systems

This RSPP applies to all safety critical processor-based signal and train control systems subject to 49 C.F.R. Part 236. This RSPP also applies to some highway-rail grade crossing warning systems that are covered under the rule as applicable and described in 234.275(a).

The following is a list of the applicable systems, which are in service on NS as of the last revision date to this document:

- None

12. APPENDIX B – Hazard Identification and Mitigation

This Appendix describes hazard identification methodologies and techniques for evaluating the proposed safety-critical processor-based signal and train control system concepts and establishing safety requirements. The objective of this activity is to clearly identify the safety requirements that must be implemented in the system design to assure future safe operation of the safety-critical processor-based signal and train control system. In general these safety analysis tasks are based on MIL-STD-882C and other standards as may be identified in the PSP.

Methodologies or techniques that are generally accepted for performing these activities include:

- Preliminary Hazards Analysis (PHA)
- Functional Fault Tree (FFT) or equivalent
- Subsystem Hazard Analysis (SSHA)
- Operating & Support Hazard Analysis (O&SHA)

B.1 Preliminary Hazards Analysis (PHA)

Preliminary Hazard Analysis (PHA) is used to identify possible hazards associated with the top-level functional requirements for the safety-critical processor-based train control system. The results of the PHA identifies high level safety hazards associated with the system and helps define mitigation measures for these hazards early in the system life cycle. The PHA shall consider the system concept, operating and support constraints and the specific operating environment where the processor-based signal and train control system will be implemented.

Documentation for the PHA shall include definition of the system concept as evaluated, description of the methodology employed, list of hazards identified, and potential mitigation measures for those hazards. The PHA is further documented through the use of analysis worksheets that list:

- Hazard identification number
- Description of the hazard

-
- Conditions (e.g., design features, operations, support requirements) that contribute to the hazard
 - Consequences or effects of the hazard
 - Resolution measures that eliminate, mitigate, or control the hazard
 - Risk ranking of the hazard in terms of hazard severity and hazard probability (RSPP, Section 3.1.2).

Sufficient references must be provided with the documentation to permit tracking of the hazard from identification through eventual resolution.

B.2 Functional Fault Tree (FFT)

A Functional Fault Tree (FFT) assists in organizing the results of a PHA to illustrate the interrelationships of the hazards, identifying the combinations of faults that contribute to the safety-critical processor-based signal and train control system hazards. These faults are represented as subsystem functions and interface with the train control system.

The development of the FFT begins with identification of a top-level safety-critical processor-based signal and train control system hazard from the PHA (e.g., train-to-train collision). Defining the hazards and/or faults that are necessary to result in the hazard defined on the previous level develops each succeeding level of the FFT. Each hazard is developed to the level of specific subsystem faults and/or interface requirements, described as terminal events. The terminal events receive further analysis during the implementation verification and validation process that examines the hardware and software implementation of the safety-critical processor-based signal and train control system. Terminal events that were not identified during previous analysis shall be tracked for future resolution.

Documentation for the FFT shall include a description of the methodology employed, explanation of hazards/faults represented by the terminal events, and a diagram showing the development of the FFT and the relationships of the terminal events to the top-level train control system hazard. Sufficient references shall be provided with the documentation to permit tracking of the faults through future analyses and eventual resolution.

Acceptable equivalent methods to the FFT may be used, such as a hierarchical list of potential accidents and faults. A hierarchical list is an experienced-based tool that lists potential accidents for a system and contributing causes to those accidents. The list shall be updated (e.g., with the results of a PHA) with new accidents and/or hazards with the introduction of new technology to remain comprehensive.

B.3 Subsystem Hazard Analysis (SSHA)

The Subsystem Hazard Analysis (SSHA) expands on the PHA to provide additional detail to the subsystem and interface level faults that contribute to safety-critical processor-based signal and train control system hazards. The SSHA may be conducted in the format of a Failure Modes, Effects, and Criticality Analysis (FMECA). The SSHA addresses subsystem failure modes, data quality and data communications, and interfaces with the existing train control systems. The SSHA must also consider the various operating modes of the safety-critical processor-based signal and train control system and specific interactions and interfaces with any existing operational and wayside equipment and conditions to examine their effects on the processor-based signal and train control system operation, operational personnel, and other parties.

Documentation for the SSHA shall describe the analysis methodology employed, the failure modes examined, how those failure modes reveal themselves in system operation, determination of failure mode risk (severity and probability rankings in this RSPP, Section 3.1.2), and resolution measures to eliminate, mitigate, or control the identified hazards. Sufficient references must be provided with the documentation to permit tracking of the hazards through future analyses and eventual resolution.

B.4 Operating & Support Hazard Analysis (O&SHA)

Operating & Support Hazard Analysis (O&SHA) examines the processes and procedures that are relied on to mitigate safety-critical processor-based signal and train control system hazards. Another objective of the O&SHA is to identify hazards that result from noncompliance with these processes and procedures. These processes and procedures include operating rules and special instructions (both normal and emergency), test and maintenance activities, and other external systems that interact with the processor-based signal and train control system. Installation errors shall be included in the O&SHA for completeness and shall be clearly identified as installation-specific hazards. Resolutions to hazards identified in the O&SHA may include requiring additional safety equipment, changes in system functionality, training, or procedures.

Documentation for the O&SHA shall describe the analysis methodology employed, the processes/procedures and/or support functions examined, how hazards reveal themselves in system operation, determination of hazard risk (severity and probability rankings), and resolution measures to eliminate, mitigate, or control the identified hazards. Sufficient references shall be provided with the documentation to permit tracking of the hazards through future analyses.

13. APPENDIX C – SAFETY VERIFICATION AND VALIDATION [49 C.F.R. Part 236, Appendix C]

The safety-critical processor-based signal and train control system design process shall include safety verification and validation activities as performed by the developer and/or NS. System safety verification and validation (V&V) comprises a set of safety activities for a system based on a collection of analyses, tests, simulations and calculations that together demonstrate compliance with all applicable safety requirements. The standards used in the verification and validation process shall be consistent with 49 C.F.R. Part 236, Appendix C.

C.1 Verification Activities

Safety verification activities encompass overall system and subsystem design, safety-critical hardware, and software. These activities include both analyses and tests that provide justification (qualitative or quantitative) for the level of safety assurance for the processor-based signal and train control system. These activities may include:

- Fault Tree Analysis (FTA);
- Failure Modes and Effects Analysis (FMEA);
- Software V&V;
- Fault Hazard Analysis (FHA);
- Safety Verification Testing.

C.1.1. Fault Tree Analysis

Fault Tree Analysis (FTA) is a deductive analysis technique for developing the contributing failures to an undesired system or subsystem fault. A comprehensive FTA shall be performed for each safety-critical processor-based signal and train control subsystem. The top-level faults for the FTA can be identified by the terminal events defined in the Functional Fault Tree development. Each of these events shall be analyzed to the level of specific hardware components and software elements required to implement the safety-

critical system function. Generally, these hardware components and software elements shall be of sufficient detail to support later analyses to define quantitative estimates of safety-critical processor-based signal and train control system safety.

C.1.2. Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is a qualitative analysis technique used to identify and analyze single point failure modes and combinations of these failure modes. FMEA shall be applied to hardware components and circuits to the level of their basic constituents. The results of the FMEA shall include identification of the single point of failure modes, the failure mode effect on the subsystem where the component is employed, and the manner in which the failure mode is detected (by component or subsystem response, testing, or other means). Failure modes that are not readily detected (i.e., are not “annunciated”) must be further investigated to determine their effect in combination with other failure modes.

C.1.3. Software V&V

Software V&V is required where the safety-critical processor-based signal and train control system is dependent on the correct and safe operation of software to implement safety-critical functions. Generally, safety-critical software shall be developed under the guidance of an approved software safety plan. This plan specifies the objectives and relationships between safety requirements, software development, software safety V&V activities, and the overall software quality assurance process.

Software V&V is comprised of a number of activities during the software development and implementation process, including analyses, inspections, walkthroughs, and database safety verification. Analyses, inspections, and walkthroughs shall be performed throughout the software development process to ensure that the outputs of each software development phase match the safety requirements for that development phase. These activities shall assure that no human errors have occurred during the software coding process.

Software safety testing is an important element of software V&V. Tests should demonstrate that each individual software module functions as intended, and that all modules are integrated into a complete product. Testing shall include all safety functions through the expected normal range of values and also at the operating

boundaries of the software design. Other features such as timing or throughput constraints shall be included in the tests.

Database Safety Verification is also necessary for the sources of data upon which the system relies. Database integrity must be ensured during initial data entry, storage, processing, updates, and communications.

C.1.4. Fault Hazard Analysis

Fault Hazard Analysis (FHA) is a bottom up analysis approach to determine the effects of low-level safety critical faults on the system. FHA includes the hardware and software modules of the system, and also ancillary equipment and interfaces such as power supplies, rail vehicle failures, and environmental conditions. The FHA confirms that the previous hazard analyses were comprehensive. Should new hazards be found as a result of the FHA, resolution actions must be specified to eliminate, minimize, or control the hazard.

C.1.5. Safety Verification Testing

Safety Verification Testing shall be performed to supplement the verification analyses and demonstrate the correct operations of safety-critical functions. Verification testing shall include both hardware and software system modules and be structured to demonstrate safe operation for expected normal operating conditions, under operating conditions that include hardware failures that were not confirmed by analysis, and under operating conditions with abnormal input conditions or other environmental conditions. The results of all tests must demonstrate the safe implementation of the safety-critical functions.

C.1.6. Validation Activities

Safety validation for a system involves the conduct of a set of activities that demonstrate the correct system has been implemented and the overall integrated system operates safely in its intended environment. Safety validation shows the integrated system performs the desired safety functions in a safe manner under all anticipated operating conditions (e.g., normal operation, hardware failures, and external influences) and that system parameters reflect the correct and actual data for the system.

Validation testing shall be conducted at the factory and in the field before actual operations begin. Testing conditions shall include normal operating conditions, conditions including random hardware failures, and conditions including abnormal inputs (such as power supply problems, inadvertent commands, and other operating environmental factors). Field tests and commissioning tests shall confirm that the system has been installed correctly and can perform safely under operating conditions.

Final Page Intentionally Left Blank