Railroad Safety Program Plan

Submitted in fulfillment of FRA Regulations Part 236, Subpart H, Section 236.905

REVISION RECORD

REV.	DATE	Description	FRA Status
1.0	June 1, 2003	ARRC draft RSPP ready for submission to FRA.	
2.0	March 5, 2007	Revised to comply with Final Rule 49 CFR Part 236H	
2.0a	May 9, 2007	Revised to consider FRA comments from March 5, 2007	
2.0b	September 11,2007	Revisions based on FRA comments of March 5, 2007	
2.0c	January 31, 2008	Revisions based on FRA comments of March 5, 2007	
2.0d	June 20, 2008	Revisions based on FRA comments of May 19, 2008	

Table of Contents

Section Title Page

1 INTRODUCTION 1-1

1.1 SCOPE AND PURPOSE 1-2
1.2 APPLICABILITY 1-2
1.3 DOCUMENT OVERVIEW 1-3
1.4 ACRONYMS AND DEFINITIONS 1-3

2 APPLICABLE DOCUMENTS 2-1

3 SYSTEM DEPLOYMENT 3-1

4 GENERAL REQUIREMENTS FOR DEVELOPMENT OF PROCESSOR-BASED SIGNAL AND TRAIN CONTROL RAILROAD SAFETY PROGRAM PLAN (RSPP) [§236.905] 4-1

4.1 ARRC SAFETY PROGRAM RESPONSIBILITIES 4-1
4.2 REQUIREMENTS AND CONCEPTS [§236.905(B) (1)] 4-2
4.2.1 Concept Requirements 4-2
4.2.2 Methods to Evaluate Behavior [§236.905(b)(1)(i)] 4-2
4.2.3 Risk Assessment [§236.905(b)(1)(ii)] 4-3
4.2.4 Risk Measurement 4-4
4.2.5 System Safety Precedence [§236.905(b)(1)(iii)] 4-6
4.2.6 Safety Assessment Process Requirements [§236.905(b)(1)(iv)] 4-6
4.3 DESIGN FOR VERIFICATION AND VALIDATION [§236.905(B)(2)] 4-7
4.3.1 Methodology 4-7
4.3.2 Standards 4-8
4.3.3 Documentation Required to Support Independent Audit of V&V 4-8
4.4 HUMAN FACTORS DESIGN REQUIREMENTS [§236.905(B)(3)] 4-10
4.5 CONFIGURATION MANAGEMENT CONTROL [§236.905(B)(4)] 4-10

5 PRODUCT SAFETY PLAN (PSP) REQUIREMENTS [§236.907] 5-1

5.1 DESCRIPTION OF THE PROCESSOR-BASED SIGNAL AND TRAIN CONTROL SYSTEM [§236.907(A)(1)] 5-1
5.2 DESCRIPTION OF RAILROAD OPERATION [§236.907(A)(2)] 5-2
5.3 OPERATIONAL CONCEPTS DOCUMENTATION [§236.907 (A)(3)] 5-2
5.4 SAFETY REQUIREMENTS DOCUMENTATION [§236.907(A)(4)] 5-2
5.5 SYSTEM ARCHITECTURE [§236.907 (A) (5)] 5-3
5.6 HAZARD LOG [§236.907 (A) (6)] 5-3
5.7 RISK ASSESSMENT REQUIREMENTS [§236.907 (A) (7)] 5-4
5.7.1 Base Case 5-4
5.7.2 Proposed System Case 5-5
5.8 HAZARD MITIGATION ANALYSES [§236.907 (A) (8)] 5-5
5.8.1 Preliminary Hazard Analysis (PHA) 5-6
5.8.2 Functional Fault Tree (FFT) 5-6
5.8.3 Operations and Support Hazard Analysis (O&SHA) 5-7
5.8.4 Mean Time to Hazardous Event (MTTHE) value 5-7
5.8.5 Phased Implementation 5-7
5.9 V&V PROCESS AND DOCUMENTATION [§236.907 (A) (9)] 5-7
5.10 SAFETY ASSURANCE CONCEPTS [§236.907 (A) (10)] 5-9
5.11 HUMAN FACTORS ANALYSIS [§236.907 (A) (11)] 5-10

5.12 Training Requirements [§236.907 (a) (12)] 5-10
5.13 Test Procedures and Equipment [§236.907 (a) (13)] 5-10
5.14 Part 236 Rules and Regulations [§236.907 (a) (14)] 5-11
5.15 Security of Safety-Critical Systems, Subsystems, & Components [§236.907(a)(15)] 5-11
5.16 Warnings and Warning Labels [§236.907 (a) (16)] 5-12
5.17 Implementation Testing [§236.907 (a)(17)] 5-12
5.18 Post Implementation Testing [§236.907 (a)(18)] 5-13
5.19 Safety-Critical Assumptions and Fallback Operations [§236.907 (a)(19)] 5-14
5.20 Incremental and Predefined Changes [§236.907(a)(20)] 5-14
5.21 Communication of Hazards [§236.907(a)(20)(d)] 5-14
5.22 ARRC System Safety Board Records 5-15
5.23 ARRC Retention of Safety Critical Control Data Routed to the Locomotive Engineer's Display 5-15

6 MINIMUM PERFORMANCE STANDARD – RESULTS OF PSP FOR PROCESSOR BASED SIGNAL AND TRAIN CONTROL SYSTEMS [§236.909] 6-1

6.1 Basis for Risk Measurement 6-1
6.2 Risk Assessment Process Options 6-2
6.2.1 Abbreviated Risk Assessment 6-2
6.2.2 Risk Assessment Basis 6-2
6.3 Risk Assessment Basis 6-3
6.4 Risk Assessment Assumptions and Sensitivity Analysis 6-4
6.5 Performance Risk Monitoring After Entering Operational Service [Rule §236.917(b)] and [Rule §236.907(a)(18)] 6-4

7 PSP REVIEW AND APPROVAL [§236.913] 7-1

7.1 Railroad Review and Approval of PSP 7-1

8 IMPLEMENTATION AND OPERATION [§236.915] 8-1

8.1 Compliance with PSP and RSPP Requirements 8-1
8.2 Restrictions on Testing of Safety-critical Processor Based Signal and Train Control Components, System, or Subsystems 8-1
8.3 System or Subsystem Failures 8-1
8.4 Informational Product Safety Plan Filing 8-2

9 SYSTEM OPERATIONS AND MAINTENANCE MANUAL [§236.919] 9-1

10 TRAINING AND QUALIFICATION PROGRAM [§236.921, §236.923, §236.925, §236.927, AND §236.929] 10-1

11 HUMAN-MACHINE INTERFACE [PART 236, APPENDIX E] 11-1

1 Introduction

This Railroad Safety Program Plan (RSPP) is the Alaska Railroad Corporation (ARRC) strategic safety planning document for the development and implementation of Processor-Based Signal and Train Control Systems. This RSPP is a living document, and may be modified to reflect changes in regulations and requests by the FRA during the RSPP approval process. Any changes to the RSPP after initial FRA approval which affect safety critical requirements will be made according to 49 CFR §236.905(d)(1) and shall be reviewed and assessed by the ARRC System Safety Board (see Section 4.1).

This RSPP is focused on the requirements of FRA Final Rule §236 Subpart H "Standards for Development and Use of Processor-Based Signal and Train Control Systems" dated March 7, 2005.

Sections 1-3 provide an introduction and overview of the RSPP.

Section 4 of this RSPP provides ARRC requirements related to safety requirements and concepts, verification and validation, human factors, and configuration management, employed by the ARRC to meet the safety goals for processor-based signal and train control systems.

Section 5 of this RSPP defines the overall requirements of the PSP as defined in §236.907. These requirements apply to all safety-critical systems which may be developed for ARRC. A Product Safety Plan Definition Document (PSPD) will be generated by ARRC to define the specific approach to be taken for the Product Safety Plan (PSP) for each major project. A PSPD for the Collision Avoidance System is provided in Ref. 2J.

Section 6 of this RSPP defines the overall requirements of the PSP as defined in §236.909. These requirements apply to all safety-critical systems which may be developed for ARRC.

Section 7 of this RSPP defines the PSP Review and approval as defined in §236.913.

Section 8 of this RSPP defines the implementation and operation requirements as defined §236.915 for products requiring a PSP.

Section 9 of this RSPP defines the system operations and maintenance manuals requirements as defined in §236.919.

Section 10 of this RSPP defines Training and Qualification Program as defined in §236.929.

Section 11 of this RSPP defines Human-Machine Interface requirements of the PSP as defined in §236 Appendix E.

A PSP is specific to a particular system and represents both the vendor's and the ARRC's safety assessment activities necessary to assure the safe design, implementation and deployment of a processor-based signal and train control system. The term vendor in this document may mean one or more companies, depending on the contractual arrangements. The PSP is viewed as a living document that includes all aspects of product safety from design through implementation and deployment. A PSP must be prepared for each type of processor-based signal and train control system (or safety critical subsystem or component) deployed by the ARRC. The ARRC shall prepare, with the assistance of the vendor, a PSP that is compliant with this RSPP and with applicable FRA regulations. ARRC will supply the required operating data. The PSP will become an ARRC document that demonstrates the safety capabilities of the processor-based signal and train control system. All documentary evidence supporting the processor-based signal and train control system PSP shall be available for review and audit by the ARRC, the ARRC's designee, and the FRA.

The ARRC shall be fully responsible for the implementation of this RSPP, the comprehensive safety design, implementation, safety verification and safety validation of the processor-based signaling and train control system, and the generation of supporting safety documentation, including compliance with all PSP requirements as defined in this document, 49 CFR 236H, and other applicable standards, requirements and regulations.

1.1 Scope and Purpose

This document describes the plan that will be used to ensure that the processor-based signal and train control system is specified, designed, built, verified, and implemented with the proper emphasis on safety, and which will ultimately demonstrate, with a high level of confidence, that the proposed processor-based signal and train control system achieves a level of safety equal to or exceeding that of the system which it replaces.

The purpose of this document is to provide uniform requirements for developing and implementing a comprehensive system safety program sufficient to identify the hazards of the processor-based signal and train control system and to impose design requirements and management controls to prevent mishaps. The aim is twofold. First, to ensure that the deployment of the processor-based signal and train control system does not result in a level of safety risk that exceeds the level of safety risk in the system being replaced; second, to eliminate hazards or reduce the associated risk to an acceptable level.

1.2 Applicability

This RSPP applies to processor-based signal and train control systems, or safety critical subsystems, or safety critical components thereof, developed and implemented subject to the provisions of §236 Subpart H "Standards for Development and Use of Processor-Based Signal

and Train Control Systems". All existing (as of the date of this RSPP) processor-based signal and train control systems are excluded unless specifically included in Section 3.

1.3 Document Overview

This document includes ARRC functional requirements, performance requirements, design guidelines, human factors, safety assurance process requirements, and verification and validation requirements for the safe operation, configuration management, deployment, and maintenance of the Collision Avoidance System in particular, and processor-based safety critical systems and subsystems in general. The document sections are listed below:

- Section 1 describes the scope of the document.
- Section 2 lists the references for this document.
- Section 3 provides a list of areas of the ARRC on which the proposed processor-based signal and train control system may be deployed.
- Section 4 presents the minimum general safety requirements for the development of processor-based signal and train control systems as defined in §236.905.
- Sections 5-11 of this RSPP defines the overall requirements of the PSP as defined in §236.907-929 and §236 Appendix E.

1.4 Acronyms and Definitions

The acronyms used in this document are defined as follows:

Acronym	Meaning
ARRC	Alaska Railroad Corporation
CAD	Computer-Aided Dispatch
CAS	Collision Avoidance System
CM	Configuration Management
ConOps	ARRC CAS Concept of Operations
CTC	Centralized Traffic Control
DoD	Department of Defense
DTC	Direct Traffic Control
FFT	Functional Fault Tree
FHA	Fault Hazard Analysis
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
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 Times to Repair
O&SHA	Operating & Support Hazard Analysis
PHA	Preliminary Hazard Assessment
PSP	Product Safety Plan
PSPD	Product Safety Plan Definition Document
RSPP	Railroad Safety Program Plan
SSB	System Safety Board
SSHA	Subsystem Hazard Analysis
V&V	Verification and Validation

The following definitions of terms are used in this document:

Terms	Definition
Component	An element, device, or appliance that is part of a system or subsystem.
Fail-Safe	A design philosophy applied to safety-critical systems such that the results of hardware failures or the effect of software error shall either prohibit the system from assuming or maintaining an unsafe state or shall cause the system to assume a state known to be safe. (IEEE-1483)
Implementation	The application of a system or subsystem to the railroad, by the action of commissioning the system or subsystem.
Hazard	An existing or potential condition that may result in an accident.
Mean Time to Hazardous Event (MTTHE)	The average or expected time that a subsystem or component will operate prior to the occurrence of an unsafe failure.
Previous Condition	Refers to the estimated risk inherent in the portion of the existing method of operation that is relevant to the change under analysis.
Preliminary Safety Analysis	A set of preliminary analyses which comprehensively identify the safety functions that the system will perform, indicate how hazards are controlled, and demonstrate that the associated risks are eliminated or mitigated.
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 processor-based signal and train control system or the previous condition.

Safety-critical	A term applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel and/or equipment; or the incorrect performance of which may cause a hazardous condition or allow a hazardous condition that was intended to be prevented by the function or system to exist.
Safety Validation	The process of determining whether a product's design requirements fulfill its intended design objectives during its development and life cycle. The goal of the validation process is to determine "whether the correct product was built."
Safety Verification	The process of determining whether the results of a given phase of the development cycle fulfill the validated requirements established at the start of that phase. The goal of the verification process is to determine "whether the product was built correctly."
Subsystem	An element of a system that, in itself may constitute a system.
System	Refers to the processor-based signal and train control system and includes all subsystems and components 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 are implemented.
Vendor	A private sector enterprise or an organizational element of ARRC engaged to provide services, develop systems, subsystems components or products used in a safety-critical processor-based signaling and train control system.
Vital Function	A function in a safety-critical system that is required to be implemented in a fail-safe manner. Note: Vital functions are a subset of safety-critical functions. (IEEE-1483)

2 Applicable Documents

The following documents were used in the preparation of this RSPP, or are referenced as required standards to be followed in the design, development and implementation of processor-based signal and train control systems. Unless 49 CFR Part 236, Subpart H requires otherwise, the latest version of each referenced document shall be used.

A. Alaska Railroad Airbrake and Train Handling Rules, latest revision.

B. Alaska Railroad Corporation Timetable, latest revision.

C. General Code of Operating Rules, Fifth Edition, Effective April 3, 2005

D. Alaska Railroad Corporation Train Dispatcher Manual, latest revision.

E. FRA Final Rule Part 236, Subpart H – Standards for Development and Use of Processor-Based Signal and Train Control Systems (published in Federal Register March 7, 2005, pages 11052 to 11108).

F. MIL-STD-882C, "System Safety Program Requirements" with Notice 1, US DoD, 13 March 1996.

G. IEEE Standard 1483-2000, "IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control", IEEE VT Society, 5 April 2000.

H. American Railway Engineering and Maintenance of Way Association (AREMA), Communications and Signals Manual - 2005, Section 17, Quality Principles; Sections 17.1.1, 17.3.1.C.15, 17.3.1.D, 17.3.1.E, 17.3.3, 17.5.1.

I. Alaska Railroad Corporation, Collision Avoidance System Concept of Operations, (ConOps), Version 5.1, September 28, 2006

J. Battelle, Alaska Railroad Collision Avoidance System Product Safety Plan Definition Document (PSPD), Version 0.4, January 24, 2008.

K. Configuration Management Standard, IEEE 828.

3 System Deployment

Deployment of the proposed safety-critical signal and train control system subject to the Rule may be on one or more of the following divisions and/or branch lines:

The Alaska Division
The Whittier Division
The Anchorage International Airport Branch
The Palmer Branch
The Suntrana Branch
The Fairbanks International Airport Branch
The Eielson Branch

The CAS will be implemented system wide on the ARRC in the State of Alaska. The following table provides the geographic locations on which the Collision Avoidance System is to be implemented.

Division or Branch	Length (miles)	Freight Trains / Day	Passenger Trains / Day Summer / Winter
Alaska: Anchorage to Seward	114.3	12	10 / 0
Whittier: Portage to Whittier	12.4	3	12 / 0
Alaska: Anchorage to Fairbanks	356.0	12	8 / 1
Anchorage Intl Airport Branch: Anchorage to end of track	2.45	0	4 / 0
Palmer Branch: Matanuska to Palmer	6.2	7	2 / 0
Suntrana Branch: Healy to End of track	1.7	1	0 / 0
Fairbanks Intl Airport Branch: Fairbanks to End of Track	10.0	2	0 / 0
Eielson Branch: Fairbanks to Eielson	28.0	4	0 / 0
Totals	**531.05**	**41**[1]	**36 / 1**[2]

Note [1]: the column totals 41. Gravel and work trains operate on more than one corridor.
Note [2]: the column totals 36. Passenger trains operate on more than one corridor.

ARRC Timetable (current version No. 134) also includes control type, mileage, and siding length.

4 General Requirements for Development of Processor-Based Signal and Train Control Railroad Safety Program Plan (RSPP) [§236.905]

This Railroad Safety Program Plan (RSPP) serves as the principal safety program plan for processor-based signal and train control systems that may be developed, acquired, and installed by the ARRC. This RSPP establishes the minimum Product Safety Plan (PSP) requirements that will govern the application of design, operating, technical, and management techniques and principles throughout the life cycle of the processor-based signal and train control system to reduce hazards and unsafe conditions. The development of a PSP will be concurrent with the design, development, deployment, and operation of the processor-based signal and train control system. The areas identified in the following subsections shall be addressed.

4.1 ARRC Safety Program Responsibilities

The ARRC Assistant Vice President of Operating Rules and Control Systems (AVP OR&CS) shall assume ultimate responsibility for the complete, correct and safe execution of all elements of this RSPP.

A System Safety Board (SSB) shall be appointed by the AVP OR&CS for the development, and implementation of any train control product or system that is required to adhere to FRA Final Rule §236 Subpart H "Standards for Development and Use of Processor-Based Signal and Train Control Systems. The SSB shall be chaired by the AVP OR&CS and shall include knowledgeable and experienced representatives of ARRC not directly associated with the development and/or deployment of the proposed safety-critical system, as well as experienced representatives of the ARRC organization involved with the proposed system's development and deployment. The SSB shall make recommendations to the ARRC AVP OR&CS for his approval.

An independent third party System Safety Engineer may be appointed to the SSB if the complexity of the proposed system warrants.

The SSB shall assure that potential hazards associated with the proposed system are adequately identified and mitigated, either by design or procedure, as appropriate. The SSB shall provide written recommendations to the AVP OR&CS regarding the acceptability of the proposed mitigations. The AVP OR&CS may accept the recommendations or return the recommendations to the SSB for further consideration and action.

In addition, the SSB shall review, assess and make recommendations for approval of all safety-related analyses and documents necessary to fulfill the requirements of 49 CFR §236.907(a); Product Safety Plan.

The documentation associated with this process shall be included in the PSP.

4.2 Requirements and Concepts [§236.905(b) (1)]

This section addresses the minimum requirements for the preliminary safety analysis of the proposed processor-based signal and train control system. The purpose of the preliminary safety analysis is to evaluate the behavior of the proposed system with regard to safe operation, safe design and verification, and human factors. The preliminary safety analysis shall be performed by the vendor in conjunction with an independent System Safety Engineer, and shall be reviewed and assessed by the ARRC SSB. The preliminary safety analysis shall include:

4.2.1 Concept Requirements

Processor-based signal and train control systems designed for ARRC for the purpose of implementing safety-critical office, wayside and train-borne functions shall be designed and implemented to be fail-safe. The safety assurance concepts used in the proposed design shall be described in a Safety Assurance Concept (SAC) document, in accordance with the standards defined in 2.G above.

4.2.2 Methods to Evaluate Behavior [§236.905(b)(1)(i)]

The following hazard identification techniques shall be used to evaluate system behavior by identifying all hazards and their causal faults which could lead to a mishap during operation with the proposed system. The highest level hazards shall be identified in a PHA and used as the top level faults of a FFT. The FFT shall be developed to the point where all functional faults associated with the operation of the proposed system are identified, including those potentially caused by the system and those potentially caused by personnel operating the railroad using the proposed system. The terminal faults of the FFT shall be grouped per subsystem, including a separate group for those faults associated with operating personnel. The terminal subsystem functional faults shall be further developed via FTA to identify potential faults in the system and subsystem implementation. The terminal faults associated with operating personnel shall be further analyzed in the O&SHA. Hazard evaluation methodologies and techniques that shall be employed include the following:

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

The PHA and O&SHA shall be developed in accordance with Mil Std 882C [Ref. 2.F]. These hazard identification methodologies shall be used to identify and establish safety requirements to eliminate, mitigate, or control potential hazards.

4.2.3 Risk Assessment [§236.905(b)(1)(ii)]

Risk assessment is applicable to two areas: 1) the comparison of risks associated with railroad operations under the proposed processor-based signal and train control system with those associated with the current operation, which the proposed system is to replace and/or enhance; and 2) the residual risks associated with human interface with the proposed system.

1) The risks associated with the operation of the proposed processor-based signal and train control system shall be assessed and shown to not exceed those associated with the system that the proposed system is intended to replace.

A fundamental objective of the PSP shall be to demonstrate that the risk associated with the implementation and operation of the Proposed [processor-based signal and train control] System is no greater than the risk associated with current train control operation (Base Case). To meet this objective, the Base Case risk assessment shall consider all potential faults associated with current train control system operation. The Proposed System Case risk assessment shall consider the quantitative analysis of potential faults associated with Proposed System functions, which shall be designed to mitigate the potential safety-critical faults in the Base Case which are related to functions performed by Proposed System and its subsystems.

The risk assessment required by §236.909 and Appendix B of the FRA Final Rule shall be implemented using Functional Fault Trees (FFTs) illustrating the faults associated with the Base Case and, separately, illustrating the inclusion of the Proposed System in conjunction with the Base Case system. In those areas where the risks associated with functions performed by the Proposed System are not self-evidently lower than the risks associated with the Base Case system performing the same function, the risks for both systems shall be quantified and compared. In this context, the term 'self-evidently lower risk' refers to the comparison of risks associated with functions designed and implemented to be fail-safe with those of the Base Case which are not implemented to be fail-safe. In this instance, MTTHE of fail-safely implemented functions is on the order of 10E9 hours, which is self-evidently higher than those in the Base Case not implemented to be fail-safe. This avoids the necessity of quantifying the risks of those Base Case functions where it would serve no purpose.

2) As described in the requirements of section 4.1.2 above, the terminal faults of the FFT of the proposed system associated with operating personnel are grouped together and further analyzed in the O&SHA. The Operating and Support Hazard Analysis shall include an assessment of the risks associated with these human interfaces to the system. The preferred approach to this evaluation is to use hazard analysis techniques that assess the risk associated with the potential human interface hazards, and provide for design or procedural protections against those risks.

Establishment of operating procedure safety requirements shall result from the determination of those human-factor related risks requiring mitigation. Safety operating procedure requirements shall be defined for human interface hazards that present a risk that cannot be accepted because

of severity and/or high probability (as per MIL STD 882C – Ref. 2.F) and thus must be eliminated by design or other explicit control measures.

4.2.4 Risk Measurement

A documented hazard risk assessment shall be performed for those hazards associated with the proposed processor-based signal and train control system which cannot be shown to have a risk less than or equal to those of the Base Case system. The risk assessment shall rank each relevant hazard in terms of severity and probability of occurrence. Once a relevant hazard is identified, an analysis of its potential severity and probability of occurrence shall be performed. The process for this analysis shall be standardized[1]. The following categories of probability and severity (taken from MIL-STD-882C) [Ref 2.F] or a SSB 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)	- Death or system loss
II.	(Critical)	- Severe injury, or major system and/or environmental damage
III.	(Marginal)	- Minor injury, or minor system and/or environmental damage
IV.	(Negligible)	- Less than minor injury, or system and/or environmental damage

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 can be described subjectively in potential occurrences per unit of time, events, population, items, or activity, and shall be ranked as follows:

A	(Frequent)	- Likely to occur frequently in an individual item; may be continuously experienced in fleet/inventory. IF(incident frequency) > 1E-3/hr.
B	(Probable)	- Will occur several times in life of an item; will occur frequently in fleet/inventory. 1E-3/hr ≥ IF > 1E-5/hr.
C	(Occasional)	- Likely to occur sometime in the life of an item; will occur several times in fleet/inventory. 1E-5/hr ≥ IF > 1E-7/hr.
D	(Remote)	- Unlikely but possible to occur in life of an item; unlikely but can be expected to occur in fleet/inventory. 1E-7/hr ≥ IF > 1E-9/hr.

[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. The SSB, 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.

E (Improbable) - So unlikely, it can be assumed occurrence may not be experienced; unlikely to occur, but possible in fleet[2]. IF ≤ 1E-9/hr.

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 ARRC will use the following predetermined matrix (Table 5.1) from MIL-STD-882C [Ref 2.F], or a SSB approved equivalent. The matrix will be used to establish hazard risk, and set priorities for resolutions that eliminate, minimize, or control the hazards.

Table 5.1. Hazard Risk Resolution Matrix

Severity → / Probability ↓	I	II	III	IV
A	UN	UN	UN	AC/WR
B	UN	UN	UD	AC/WR
C	UN	UD	UD	AC
D	UD	UD	AC/WR	AC
E	AC/WR	AC/WR	AC/WR	AC

Codes: UN - Unacceptable; AC/WR - Acceptable with review by ARRC management
UD - Undesirable; AC – Acceptable without review

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 relevant hazards that present a risk that cannot be accepted because of severity and/or high probability ("unacceptable" or "undesirable" risk index in Table 5.1) and thus must be eliminated by design or other explicit control measures. 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 ARRC.[3]

[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.

[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 [Ref 2.F].

4.2.5 System Safety Precedence [§236.905(b)(1)(iii)]

The vendor shall follow the order of precedence for satisfying the processor-based signal and train control system safety requirements and resolving identified hazards per this RSPP as follows:

a) Design for minimum risk. Eliminate hazards through design. Minimize or eliminate the use of human input for safety-critical 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, reduce the associated risk to an acceptable level through design selection and proper implementation using Safety Assurance Concepts. The ARRC SSB shall assess the level of mitigation of a hazard achieved by designing for minimum risk and make recommendations for approval or disapproval to the AVP OR&CS.

b) 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. The ARRC SSB shall assess the level of mitigation of a hazard achieved by incorporating safety devices and make recommendations for approval or disapproval to the AVP OR&CS.

c) 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. The ARRC SSB shall assess the level of mitigation of a hazard achieved by providing warning devices and labels and make recommendations for approval or disapproval to the AVP OR&CS.

d) Develop procedures and training. Procedures and training shall only be used with prior ARRC 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. The ARRC SSB shall assess the level of mitigation of a hazard achieved by developing operating procedures and training and make recommendations for approval or disapproval to the AVP OR&CS.

4.2.6 Safety Assessment Process Requirements [§236.905(b)(1)(iv)]

The proposed fail-safe processor-based signal and train control system shall be implemented and managed using a comprehensive safety assurance process that addresses the life cycle of the

system. This safety assurance process shall be focused on identifying and resolving hazards associated with the system throughout its life cycle. Evidence that the safety assurance process will meet the requirements established by ARRC and applicable federal regulations shall be based upon the ARRC SSB review of system safety documentation and acceptance by the AVP OR&CS.

The vendor shall execute and document this process as part of the PSP where appropriate. The framework of this safety assurance process focuses on the following elements.

- Performing safety verification activities to assure system fail-safe implementation of safety-critical functions as defined by IEEE 1483-2000 [Ref. 2.G] and AREMA requirements [Ref. 2.H].
- Identifying potential hazards throughout the system life cycle.
- 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.
- Performing safety validation on all safety-critical functions, as implemented, to demonstrate and assure system safety.
- Monitoring testing and system operations to ensure achievement of safety requirements.

4.3 Design for Verification and Validation [§236.905(b)(2)]

The 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 analyses, tests, simulations and calculations that together demonstrate compliance with all applicable safety requirements.

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 and undesirable hazards have been mitigated or eliminated.

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. These safety validation and verification activities establish the technical evidence of the processor-based signal and train control system safety.

To minimize the extent of safety validation and verification required to satisfy the requirements of this RSPP, safety-critical functions shall be designed to be isolated or partitioned to operate as independent of other non-safety-related functions to the greatest extent possible.

4.3.1 Methodology

The PSP shall identify the safety validation and verification methods for the preliminary safety analysis, the initial development process and future incremental changes, including standards to

be used in the validation and verification process, consistent with Appendix C – Safety Assurance Criteria and Processes.

4.3.2 Standards

The safety validation and verification activities shall incorporate requirements and guidance from existing standards for safety validation and verification of hardware and software consistent with Appendix C of FRA Rule Part 236H – Safety Assurance Criteria and Processes. Applicable standards will be identified in the PSP and adhered to throughout the safety validation and verification process.

Standards required to be followed in the design, implementation, safety verification and validation of the fail-safe processor-based signal and train control system are:

- FRA Final Rule, 236H [Ref. 2.E];
- Mil Std 882C [Ref. 2.F];
- IEEE 1483-2000 [Ref. 2.G]; and
- AREMA Part 17 [Ref. 2.H].

The processor-based signal and train control system PSP shall clearly identify any additional standards and requirements that will be used in the design, development, installation, and testing of the product. A copy of any non-published standards shall be included with the PSP.

Use of standards not identified above shall require approval of the ARRC AVP OR&CS.

4.3.3 Documentation Required to Support Independent Audit of V&V

All safety V&V activities shall be sufficiently documented to record the specific activities undertaken and their results, and shall provide a credible audit trail for project team review and/or a possible independent, third party confirmation 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 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.

Third party assessment documentation per Appendix D of 236H may be required by the ARRC to provide an independent evaluation of the extent to which safety design practices were used during the development and testing phase. General requirements applied to third party assessments include:

- Preservation of the reviewers' independence and maintaining the vendor's proprietary rights.
- Access to documentation, and attendance where possible at design reviews and "walkthroughs" deemed necessary.

The following levels of third party evaluation and functionality may occur:

Preliminary Level:

- Evaluation of the processes used, including documentation of any identified safety vulnerabilities that are not mitigated.
- Evaluation of the ARRC RSPP and PSP.

Functional Level:

- Review of the Preliminary Hazard Analysis (PHA), Functional Fault Tree (FFT), Fault Tree Analysis (FTA), and the Fault Modes Effects Criticality Analysis (FMECA) for correctness, completeness and compliance with the ARRC RSPP.

Implementation Level:

- The third party shall randomly select various safety-critical software modules, of sufficient quantity to provide a high level of confidence that the total is in compliance with the RSPP, for audit to verify that RSPP requirements are followed.

Final Report:

- The third party shall evaluate and comment on the installation plan and test procedures.
- The third party shall prepare a final report of the assessment that contains the following:
    - An evaluation of the adequacy of the PSP, including the vendors MTTHE and risk estimates, and the vendor's confidence interval in the estimates; the vulnerabilities which were not adequately mitigated, including the method by which ARRC would assure safety in the event of hardware or software failure, and the method by which ARRC addresses comprehensiveness of the design for the requirements of the operation;
    - Identifying each vulnerability and clearly stating the position of the vendor and ARRC relating to the vulnerability;
    - Identifying any denied, incomplete, or inadequate documentation;
    - Listing each RSPP procedure or process which was not properly followed;

- An evaluation of the software verification and validation procedures for the processor-based signal and train control system safety-critical applications;
- Identifying the methods employed by the vendor in developing safety-critical software.

4.4 Human Factors Design Requirements [§236.905(b)(3)]

The PSP shall identify the process used during the processor-based signal and train control system development to identify human factors issues and develop design requirements that address all functions involving human interface This activity is limited to safety-critical functions and data input, including; train cab layout, interface with cab displays and data input mechanisms, and operator interface with CAD and radio systems. The PSP shall contain a human factors analysis of human-machine interface (HMI) safety functions performed by humans while the system is in operation.

The PSP will identify human factors issues in the O&SHA and document the manner in which the design of the processor-based signal and train control system addresses each human factor issue identified. The vendor must consider the general functions identified in Appendix E of 49 CFR 236H.

The human factors requirements of the processor-based signal and train control system shall be consistent with the ARRC operating practices and with railroad rules and procedures for safe operation. Any proposed use of additional railroad rules and/or procedures for safe operation requires prior approval by the ARRC SSB.

4.5 Configuration Management Control [§236.905(b)(4)]

Methods for configuration control and associated documentation shall accompany design and development of the 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 the system. Such identification will be provided in documents and databases using a consistent symbol, word or unique character that means “safety-critical”.

A Configuration Management Plan (CMP) shall establish the CM practices to be used on all hardware, software and documentation developed for the processor-based signal and train control system. ARRC will review and approve the vendor’s proposed Configuration Management Plan to ensure that it is comprehensive. The CMP shall include methodologies used to track changes, request changes, and summarize the impact analyses for hardware and software changes within the safety-critical signal or train control system. These control management methodologies shall be approved by the ARRC.

The Configuration Management Plan shall conform to Ref. 2.K, IEEE 828, or shall be equivalent to IEEE 828, as determined by the ARRC SSB.

Functional changes to software embodied in the processor-based signal and train control system after initial installation and test shall be subject to review by the ARRC SSB, which will act as a change review board.

Configuration management is a process to:

- Identify and document the functional and physical characteristics of configuration items, including: a Hardware Management Control Plan, a Software Management Control Plan and a Management Control Plan for supporting documentation crucial to the operation.
- Audit the configuration items to verify conformance to specifications, standards, and other contract requirements.
- Control changes to configuration items and their related documentation.
- Record and report information needed to manage configuration items effectively, including the status of proposed changes and the implementation status of approved changes.
- Report status of the product or system configuration to ARRC as necessary.

5 Product Safety Plan (PSP) Requirements [§236.907]

The ARRC shall prepare, with the assistance of the vendor, a Product Safety Plan (PSP) compliant with this RSPP and with applicable FRA regulations for the equipment included in the processor-based signal and train control system. The PSP shall describe the processor-based signal and train control system in detail, provide evidence of complete safety verification and safety validation, and include acceptable procedures for the implementation, testing, and maintenance. The PSP shall contain the minimum requirements described in the subsections listed below. A Product Safety Plan Definition document (PSPD) will be generated by ARRC describing the railroad's approach to complying with §236.907 of the Rule.

The minimum requirements described below include various analyses, test results, and other documentation that support the ARRC safety program and activities. This 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 produced by and/or required of the vendor supporting the PSP, shall be available for review and audit by the ARRC and the ARRC's designee. The confidentiality of proprietary information submitted in support of the PSP by the vendor shall be addressed among the vendor, ARRC and the FRA, regarding submission to the FRA of supporting material.

The following subsections shall be considered as the minimum requirements for the PSP.

5.1 Description of the processor-based signal and train control System [§236.907(a)(1)]

The processor-based signal and train control system PSP shall contain a complete description of the system, including a list of the components and their physical relationship. This description shall include the following minimum requirements:

- General description of the processor-based signal and train control system and its role in the overall train control system operation, including interfaces and interactions with existing systems and/or equipment.
- Physical description of the processor-based signal and train control system including identification of any subsystems and/or modules that makes up the processor-based signal and train control system.
- Descriptions of individual subsystems and/or modules including their function within the processor-based signal and train control system.

5.2 Description of Railroad Operation [§236.907(a)(2)]

The PSP will describe the types of railroad operations where the processor-based signal and train control system may be used. The processor-based signal and train control system may be used in both DTC and CTC territories and shall be safe regardless of train volume, load volume, passenger train volume, hazardous material volume, operating speeds, and other physical and operating characteristics. ARRC will include a description of the relevant ARRC physical infrastructure and current and planned operations for the ARRC Divisions involved. This section of the PSP will also describe the maximum train volume, train frequency, operating speed, and other physical infrastructure features as applicable, for which the system is designed.

ARRC shall provide information describing the behavior and physical characteristics of the railroad territory applicable to the proposed safety-critical system for inclusion in the ConOps document. This information shall include traffic volumes, track configuration, detailed infrastructure descriptions, territory control type and other necessary characteristics.

5.3 Operational Concepts Documentation [§236.907 (a)(3)]

The processor-based signal and train control system PSP shall describe the operational concepts, the functionality of the various subsystems and/or modules, and information flows within the System. This Concept of Operations description will include the processor-based signal and train control system operational concepts as defined for both normal and abnormal operating conditions.

The ConOps document plays a central role in defining the complete set of functions performed in operating the railroad, forming the basis of discovering and identifying all the potential hazards associated with railroad operations under the proposed system. The high level identification of potential hazards in the PHA and their subsequent expansion in the FFT will rely heavily on the completeness of the description of operational scenarios and other information contained in the ConOps. To this end, traceability will be maintained between the ConOps and the PHA and FFT.

5.4 Safety Requirements Documentation [§236.907(a)(4)]

This section of the PSP shall comprehensively identify the requirements necessary for the safe operation of the processor-based signal and train control system for its intended application. Each safety requirement shall be further defined by the specific functions that must be implemented in the specific subsystem or component of the processor-based signal and train control system in order to satisfy the given safety requirement.

This document shall specify the detailed functional safety requirements for the proposed system and each subsystem. The main sources of these safety requirements shall be derived from the terminal functional faults identified in the FFT. As stated above, the FFT identifies all functional faults, partitioned by subsystem, which could precipitate hazards and/or mishaps in railroad

operations using the proposed system. The FFT terminal faults then represent the lowest level functional origin of any hazard and/or mishap. Therefore, the complete set of functional safety requirements for each subsystem shall be identified as requirements which prohibit the occurrence of each FFT terminal faults.

Both hardware and software safety requirements are identified as necessary. Each safety requirement listed at the subsystem functional level shall be used to trace to one or more detail design requirements implemented in the safety-critical subsystems of the proposed system in order to satisfy the given safety requirement.

5.5 System Architecture [§236.907 (a) (5)]

The PSP shall describe the processor-based signal and train control system architecture and how the system architecture satisfies each system safety requirement at the overall system level. The system architecture should cover both software and hardware aspects which identify the protection developed against random hardware faults and systematic errors. These System Safety Concepts shall be identified as part of the overall architecture of the system in order to support safe operation.

The system architecture document shall describe, at a high level, how safety is achieved by allocating safety-critical functions to subsystems, which shall perform those functions fail-safely.

5.6 Hazard Log [§236.907 (a) (6)]

The Hazard Log shall be used as a tool to track the mitigation of hazards associated with all interfaces to the proposed system elements. Note that hazards mitigated by the vital subsystems themselves shall be comprehensively identified in the FFT, and tracked via the Functional Safety Requirements Specification and the various Safety Verification documents, and are not included in the Hazard Log.

The Hazard Log provides a specific description of the hazards that must be addressed throughout the life cycle of the proposed system as derived from a review of the functionality, operating methods, and the hazard analysis. The primary sources for the hazard log are the PHA and O&SHA. Other key hazards requiring mitigation may be identified from design reviews and testing, and these will be added in the same format in the Hazard Log for tracking.

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

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

4. Risk ranking of the hazard stated threshold level (residual hazard risk index) that, if exceeded, would be unacceptable. In addition, hazards with a hazard severity ranking of I or II (potential for death, system loss, or serious injury) are designated and identified as a Safety Critical Item.
5. Proposed resolution for the hazard.
6. Assignment of responsibility for the resolution action to a program function/organization.
7. Status of the hazard resolution action, including actions taken, date of actions, review and approval of the action, references to source documents supporting the action, and recommendations of the ARRC SSB.
8. Notation of whether the hazard is OPEN (requiring further action) or CLOSED (resolution action(s) complete and approved by ARRC SSB).

Each hazard description shall include a designation of Safety-Criticality. Safety Critical Items will require completion of the defined resolutions prior to concluding the safety program. The Hazard Log is a living document that is updated throughout the project. As actions are completed to resolve the specific hazards identified, the action and date are noted. Closure for each hazard in the Hazard Log shall be required for submission of the log in the PSP. Closure of all hazards for the proposed system, as indicated in the PSP Hazard Log submission, shall be required prior to the system entering revenue service.

The Hazard Log shall be maintained throughout the life of the system. Hazards identified subsequent to the system operating in revenue service shall be tracked in the Hazard Log and evidence of hazard mitigation provided. The closure of all hazards and the effects of open hazards on rail operations shall be monitored by the ARRC SSB.

5.7 Risk Assessment Requirements [§236.907 (a) (7)]

The PSP shall include a risk assessment of identified hazards consistent with the risk assessment strategy defined in Section 4.2.2 of this RSPP and part 236.907 (a) (7), and Appendix B of the Final Rule, Part 236H.

5.7.1 Base Case

The Base Case Risk Analysis shall identify the risks associated with current system operation. The risk analysis shall be in the form of a FFT, in which all faults associated with Base Case operation are structurally arranged, indicating the comprehensive fault sets which could precipitate each hazard.

Note that the risk assessment approach described here differentiates between ‘risk analysis’ and ‘risk assessment’. Risk analysis is used to comprehensively identify the risks associated with

each case, while the risk assessment is a comparison of the risks identified in each case with a quantitative assessment of the difference in risk between the two cases.

In this approach, a risk analysis is performed on the Base Case which hierarchically identifies all mishaps, their associated hazards, and all potential faults (by both human and machine), using an FFT. This FFT is easily extracted from the system FFT, which identifies both the fault set associated with the Base Case as well as those associated with the proposed system mitigations.

Reference is made to procedural mitigations of faults as defined in the O&SHA.

5.7.2 Proposed System Case

The Proposed System Case Risk Analysis shall identify the risks associated with operation of the proposed system, including all system elements which are introduced as mitigations to hazards identified in the Base Case. The risk analysis will be in the form of an FFT, in which all faults associated with Proposed System Case operation are structurally arranged, indicating the comprehensive fault sets which could precipitate each hazard.

The risk analysis performed on the Proposed System Case shall also hierarchically identify all mishaps, their associated hazards, and all potential faults (by both human and machine), using an FFT. This FFT shall be extracted from the system FFT, which identifies both the fault set associated with the Base Case as well as those associated with the Proposed System mitigations.

Reference is made to procedural mitigations of faults as defined in the O&SHA.

Subsets of the FFTs of the Base Case and the Proposed System Case which contain those hazards in the Base Case which are mitigated by Proposed System elements, shall be extracted. Quantitative data in the form of MTTHE values representing the likelihood of occurrence of faults associated with Proposed System mitigations will be introduced. MTTHE values representing the likelihood of occurrence of the corresponding Base Case faults will also be derived, where necessary. In each case where the FFT shows a fault which can be caused by the Base Case system element AND by a Proposed System element, a quantitative assessment will be made. It shall be demonstrated that in each instance, mitigation provided by the Proposed System reduces the risk of the occurrence of that fault.

5.8 Hazard Mitigation Analyses [§236.907 (a) (8)]

The PSP shall employ hazard mitigation analyses to document the process and techniques employed to identify and mitigate the consequences of various hazards. All hazards addressed in the system hardware and software, including failure mode, possible cause, effect of failure, and remedial action shall be listed in a hazard log. Hazards associated with the processor-based signal and train control system will be identified, with particular focus on hazards found to have significant safety effects. Steps taken to identify, eliminate, mitigate, or control hazards shall be

documented. Mitigation of hazards shall follow the rules for System Safety Precedence defined in Section 4.2.4 of this RSPP.

Methodologies or techniques accepted for performing these activities include:

5.8.1 Preliminary Hazard Analysis (PHA)

The Preliminary Hazard Analysis (PHA) is used to identify possible hazards associated with the top-level functional requirements for the processor-based signal and 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 a hazard log that lists:

- 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 assessment of the hazard in terms of hazard severity and hazard probability (RSPP, Section 4.1.2).

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

5.8.2 Functional Fault Tree (FFT)

A Functional Fault Tree (FFT) assists in organizing the results of a PHA to establish and trace the link between the processor-based signal and train control system and component failures to the hazards resulting from these failures. The documentation must illustrate the interrelationships of the hazards, identifying the combinations of faults that contribute to the processor-based signal and train control system hazards. These faults are represented as subsystem functions and interfaces with the processor-based signal and train control system.

The development of the FFT begins with identification of a top-level 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 processor-based signal and train control system. Terminal events identified after the initial analysis shall be tracked for future resolution.

The terminal fault events of the FFT shall be grouped according to the system entity required to protect against the occurrence of those faults. System entities include both subsystems and operating and support procedures. Those faults associated with operations and support shall be further analyzed in the O&SHA.

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.

5.8.3 Operations and Support Hazard Analysis (O&SHA)

An Operations and Support Hazard Analysis shall be performed on hazards associated with train control and maintenance operations. Sources of hazards associated with operations and support shall include the related terminal fault events of the FFT and from the analysis of human factors.

The O&SHA shall describe each hazard and propose mitigations in terms of procedural requirements. Closure of each hazard shall require evidence that the associated operating or maintenance procedure meet the requirements specified in the O&SHA.

5.8.4 Mean Time to Hazardous Event (MTTHE) value

An MTTHE value must be calculated for each processor-based signal and train control system subsystem and component, including the safety-critical behavior of the integrated hardware/software subsystem and/or component.

5.8.5 Phased Implementation

In the event that the processor-based signal and train control system is not fully implemented at the commencement of revenue service, a Phased Implementation Hazard Analysis shall be generated which defines the hazards associated with revenue service operations without all aspects of the system installed.

Hazards identified shall be incorporated into the Hazard Log for tracking by the ARRC SSB.

5.9 V&V Process and Documentation [§236.907 (a) (9)]

The PSP shall describe the verification and validation (V&V) activities performed during the development and define the V&V process necessary to safely deploy the processor-based signal and train control system. The PSP shall describe how the following Rule 236H Appendix C

subject areas are addressed directly, addressed using other safety criteria, or are not applicable. Third party V&V assessment requirements, if necessary, are identified in Section 4.2.3 above.

a) Minimum criteria and processes for safety analyses conducted in support of the PSP are documented in Rule 236H Appendix C. The analysis shall:
   1. address each paragraph of Appendix C, explaining how the requirements were satisfied or why they are not relevant; or
   2. employ a validation and verification process pursuant to paragraph c of §236.907 (a) (9).

b) The vendor shall address each of the following safety considerations. In the event that any of the principles are not followed, the PSP shall state both the reason(s) for departure and the alternative(s) utilized to mitigate or eliminate the hazards associated with the design principle not followed.

   1. Normal operation: The system must demonstrate safe operation with no hardware failures under normal operating conditions (all safety-critical functions must be performed properly) with proper inputs and within the expected range of environmental conditions. Operations with the processor-based signal and train control system must not depend upon the correctness of actions or procedures used by operations personnel. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

   2. Systematic Failure: The processor-based signal and train control system must be shown to be free of unsafe systematic failure (those which can be attributed to human error that could occur at various stages throughout product development). This includes unsafe errors in the software due to human error in software specifications, design and/or coding; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

   3. Random failure:
      a. The processor-based signal and train control system must be shown to operate safely under conditions of random hardware failure. Frequency of attempted restarts must be considered in the hazard analysis.
      b. The processor-based signal and train control system shall allow no single point failures that can result in hazards categorized as unacceptable or undesirable.
      c. If one non-self-revealing failure combined with a second failure can cause a hazard that is categorized as unacceptable or undesirable, then the second failure must be detected and the processor-based signal and train control system must achieve a known safe state before falsely activating any physical appliance.

4. Common Mode failure: The processor-based signal and train control system, as defined in 236H Appendix C (4), must protect against unsafe conditions that result from two or more subsystems or components intended to compensate one another to perform the same function all fail by the same mode.

5. External Influences: The processor-based signal and train control system must be shown to operate safely when subjected to different external influences, including electrical influences, mechanical influences, and environmental conditions.

6. Modifications: Safety must be ensured following modifications to the hardware and/or software.

7. Software: Software faults must not cause hazards categorized as unacceptable or undesirable.

8. Closed Loop Principle: The processor-based signal and train control system design must require positive action to be taken in a prescribed manner to either begin operation or continue operation.

c) The standards employed for verification and/or validation of the processor-based signal and train control system are subject to this subpart and must be sufficient to support achievement of the applicable requirements of this subpart.

IEEE-1483-2000 shall be considered the primary standard for Safety Verification.

Other acceptable standards for verification and validation are:
1. The U.S. Department of Defense Standard 882C (System Safety Program Plan Requirements; Jan. 19, 1993), which is recognized as providing appropriate risk analysis processes for incorporation into verification and validation standards.
2. The standards identified in 236H Appendix C, paragraph c, subparagraph (3).
3. Unpublished standards that achieve the requirements of 236H Appendix C.

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

5.10 Safety Assurance Concepts [§236.907 (a) (10)]

The processor-based signal and train control system documentation provided by the vendor shall include a complete description of the safety assurance concepts used in design, including an explanation of the design principles and assumptions. The description shall be in the form of a Safety Assurance Concepts document, meeting the requirements of the applicable sections of IEEE 1483-2000 (Ref. 2.G).

5.11 Human Factors Analysis [§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 processor-based signal and train control 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 processor-based signal and train control system to enhance or preserve safety, and an analysis describing how human factors covered in §236.931 are addressed directly, addresses using other safety criteria, or are not applicable.

The scope and techniques of the human factors analysis shall be adequate to show that the product or system substantially complies with all of the applicable requirements of FRA regulations subpart H, Appendix E.

The scope of this part shall be limited to those functions identified in the hazard analyses (PHA and FFT) which employ humans in the correct execution of safety critical tasks. Likewise, this part is interpreted as limited to those HMIs involved in the execution of those tasks.

A minimum of two types of analyses are required; 1) an Operations and Support Hazard Analysis (O&SHA) which describes and analyzes those faults identified in PHA and FFT that are human related (the O&SHA will identify and define the requirements of the procedures which will be cited as mitigations to the human-related hazards), and 2) a Human Factors Analysis, in which the risks associated with the human performance of safety-related functions will be derived.

5.12 Training Requirements [§236.907 (a) (12)]

ARRC shall document in the PSP the training requirements necessary to ensure the safe operation, maintenance, and repair of processor-based signal and train control systems. These training requirements will address installation, normal and abnormal operation, repair, modification, and testing of the system, and will be developed jointly by the vendor and the ARRC. The PSP shall identify the intended audience for each training requirement.

5.13 Test Procedures and Equipment [§236.907 (a) (13)]

The PSP shall document test procedures and identify requirements for test equipment (as needed) for the maintenance of the processor-based signal and train control system equipment to ensure safe operation. 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, must be consistent with system needs, and shall contain explanation of any deviation from the recommendations of vendor of the equipment. The following types of testing activity shall be included under this requirement:

- Qualification testing designed to demonstrate that the processor-based signal and train control system is suitable for a particular application, performed at the factory, or on an operating line of the railroad.
- Installation testing designed to demonstrate that the equipment has been installed correctly.

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.

The O&SHA will define requirements for procedures necessary to mitigate human-related hazards associated with safety-critical functions. The procedures themselves are developed under this part and used for operation and maintenance training of ARRC personnel.

The Operation and Maintenance Procedures document may include procedures for all ARRC operations and maintenance activities involving the proposed system, however those activities which pertain to identified safety-related operations and safety-related maintenance procedures will be clearly identified. As required, the safety-related operations procedures will be succinct and comprehensive, and the safety-related maintenance procedures will clearly describe the methods to be used.

Note: Safety Validation of the proposed system equipment is addressed in Section 5.17 of this RSPP.

5.14 Part 236 Rules and Regulations [§236.907 (a) (14)]

The PSP shall list the rules and regulations of the other subparts (A-G) of Part 236 that do not apply or are satisfied by the processor-based signal and train control system using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled per §§234.275 and 236.901(c). 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.

5.15 Security of Safety-Critical Systems, Subsystems, & Components [§236.907(a)(15)]

The PSP shall describe security measures for the protection of the processor-based signal and train control system. 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 system. 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.

This section shall contain an analysis of the vulnerability of proposed system operation to corruption by unauthorized persons, causing either unintended operation or causing all or part of the system to be inoperable, and the design measures taken or procedures implemented to reduce or eliminate that vulnerability.

5.16 Warnings and Warning Labels [§236.907 (a) (16)]

The PSP shall include descriptions of all warnings and warning labels that are provided in system manuals or placed on system equipment. These warnings shall address hazards to personnel safety and operations safety when inspecting, testing, or maintaining the processor-based signal and train control system equipment.

As noted in the System Safety Precedence called for in Section 4.1.3 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 vendor training for users of the processor-based signal and train control system and/or its subsystems.

5.17 Implementation Testing [§236.907 (a)(17)]

A complete Test Plan describing all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated shall be developed. The Test Plan, test descriptions and results shall be included in the PSP.

The Test Plan shall contain descriptions of and procedures for pre-implementation factory testing, field-testing, and cutover testing that will demonstrate that the safety-critical requirements are met and the safety-critical hazards are mitigated to the appropriate level. Detailed field testing procedures shall be used to assure that the processor-based signal and train control system is properly installed and documented and identifies measures to provide for the safety of train operations during field test and cutover. Such pre-implementation testing shall be shown (by requirement and/or hazard tracing) to verify the mitigation of all identified hazards by the processor-based signal and train control 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.

The Test Plan shall contain test procedures which address two activities; 1) safety validation of all vital functions implemented by the proposed system and subsystems, and 2) procedures for installation, testing and cutover which protect the safety of the personnel and equipment involved.

The vendor shall provide the ARRC with the Test Plan and associated procedures developed per this requirement, and obtain approval of the Test Plan and procedures from ARRC, prior to conducting the testing. ARRC shall provide to the FRA Senior Test Monitor all test plans and procedures 30 calendar days prior to those tests requiring FRA monitoring. Test plans for this requirement may be subject to review and approval by the FRA.

Section 5.9 of this RSPP addresses safety verification, i.e., verification that all safety requirements have been properly specified and implemented in each of the subsystems, and that the implementation of those functions by the subsystems has been demonstrated to be fail-safe.

This PSP part shall address safety validation; demonstrating, through validation methods including testing, that those vital and safety-critical functions, when performed by their respective subsystems, result in safe operation. That is to say, safety validation demonstrates that the fundamental logic of those functions is correct and contributes to and protects the safety of the system during operation.

5.18 Post Implementation Testing [§236.907 (a)(18)]

This PSP part shall address two activities; 1) identification of all elements of the proposed system that require post implementation measures to be taken to ensure their continued safe operation, and specification of the particulars of those measures, and 2) ARRC procedures which will implement those measures and maintain the appropriate records.

The PSP shall identify a complete description of all post implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety critical tolerances are not compromised over time, over use, or after maintenance is performed. In addition, [§236.907 (a)(18)] section ii requires a complete description of each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, test, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards will be provided.

The vendor shall provide the ARRC with the test plans and procedures developed per this requirement, and obtain approval by the appropriate official of the railroad, prior to conducting the testing. ARRC shall provide to the FRA Senior Test Monitor all test plans and procedures 30 calendar days prior to those tests requiring FRA monitoring. Test plans may be subject to review and approval by the FRA.

5.19 Safety-Critical Assumptions and Fallback Operations [§236.907 (a)(19)]

Unavailability of all or portions of the proposed system may require different modes of operation (fallback operations), and that there may be distinct hazards associated with fallback operation.

This PSP section shall contain a description of all fallback operations anticipated in the event of failure or abnormal operation of the proposed system. Scenarios defining operational situations where fallback operations are required shall be developed in the ConOps, and their associated hazards shall be identified and developed in the PHA and FFT.

Descriptions of all safety-critical fallback situations shall be included in the Dispatcher Operations Manual and the Train Operator Operations Manual. This PSP section shall summarize and reference fallback operations defined in the aforementioned manuals and demonstrate that potential system failures are covered by the set of fallback operations.

5.20 Incremental and Predefined Changes [§236.907(a)(20)]

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 PSP section 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.

5.21 Communication of Hazards [§236.907(a)(20)(d)]

The PSP shall specify all contractual arrangements for hardware and software supplied for the proposed system so that immediate notification to the ARRC will be provided for any and all safety-critical software updates and/or revisions to the system, subsystems or components. This notification shall include the reason for the change and interim remediation for any and all identified hazards that may affect the safe and proper operation of the system.

All proposed hardware and/or software changes shall be subject to review and approval by the ARRC SSB.

The PSP shall specify actions to be taken by ARRC upon notification of such a safety-critical upgrade or revision, as well as any actions to be taken by ARRC prior to their installation. These procedures shall be consistent with the criteria defined in §236.915(d).

The PSP shall contain configuration and revision control measures designed to ensure that safety functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any change.

5.22 ARRC System Safety Board Records

Written records of the procedures, actions and recommendations of the ARRC SSB as described in RSPP Section 4.1 above, shall be included in this section of the PSP.

5.23 ARRC Retention of Safety Critical Control Data Routed to the Locomotive Engineer's Display

The Vendor shall comply with §229.135(b)(3)(xxv) with regards to retention of safety critical data on a certified crashworthy memory module for any locomotives or DMUs to act in the lead position that are ordered after October 1, 2006 or placed into service on or after October 1, 2009. The Vendor will not be required to supply certified crashworthy memory for all other locomotives until a commercially available solution is developed.

For CAS, the retention of safety critical train control data routed to the locomotive engineer's display shall be maintained in the OBC memory for a minimum of 48 hours. The locomotive event recorders and the OBC memory will each have a checkpoint entered in their logs to provide a method to calibrate the safety critical control data with the other required train data elements required in 229.135(B)(3). The retention of the Safety Critical data will meet the requirements specified in §229.135(b) and will be described in further detail in the PSP.

6 Minimum Performance Standard – Results of PSP for Processor Based Signal and Train Control Systems [§236.909]

The safety analysis included in the Product Safety Plan shall establish, with a high degree of confidence[4], that the implementation of the safety-critical processor-based signal or train control system, subsystem or product shall not exceed the risk presented by the previous condition. Alaska Railroad shall ensure that this performance standard is achieved, and will make available to the Federal Railroad Administration the analysis and documentation supporting the evaluation.

6.1 Basis for Risk Measurement

The Product Safety Plan shall describe the risk assessment methodology to be used, as required by Section 5.7 of the Railroad Safety Program plan and described in section 4.2. The methodology shall meet the guidelines of the FRA rule, as stated in 49 CFR §236 Part H Appendix B. If the Vendor proposes an alternative assessment method, the Vendor shall demonstrate to Alaska Railroad that the risk assessment methodology is suitable in the context of the product being supplied. Alaska Railroad shall forward the method to the Federal Railroad Administration Associate Administrator for Safety for approval. In this case, written FRA approval must be obtained prior to the Vendor performing risk assessment.

The scope of the risk comparison shall include only those aspects of the overall train control system that will be impacted by the implementation of the new product (e.g., processor-based signal and train control system). The risk assessment shall determine the change in risk over the product's life cycle after the implementation of all mitigating measures as specified in the Product Safety Plan.

The previous condition shall be adjusted to reflect any associated impact on risk, if changes in the physical or operating conditions on the railroad are planned, per 49 CFR

[4] High degree of confidence means that there exists credible safety analysis which is sufficient to persuade a reasonable decision-maker that the likelihood of the proposed condition associated with the new product being less safe than the previous condition is very small (remote).

§236.909(e)(2) and (3). A common risk metric shall be used to allow comparison of the safety performance of the existing condition and the new system under the (adjusted if necessary) operating scenario. The risk assessment of the product will be based on the potential hazardous modes of failure, and the degree to which the system minimizes the risk by controlling faults and failures. Faults and failures that must be considered include the hardware failures, software errors, human errors, and external influences.

6.2 Risk Assessment Process Options

The risk assessment for the product contained in the Product Safety Plan shall comply with one of the following two requirements:

6.2.1 Abbreviated Risk Assessment

An abbreviated risk assessment demonstrates that the resulting MTTHE for the safety-critical processor-based signal or train control system is greater than the MTTHE for the existing method of operation (previous condition). This determination must be supported by credible safety analysis and concurrence from the Alaska Railroad AVP OR & CS that an abbreviated risk assessment is acceptable for the subject system. Use of AREMA standard development may be used on a case-by-case basis for abbreviated risk assessment as designated by Alaska Railroad and where appropriate.

If the system or product being introduced performs the same function as the previous condition, an abbreviated risk assessment may be applied by the Vendor if, in addition, the product: (1) the proposed processor-based signal or train control system introduces no new hazard, (2) the severity of each hazard associated with the previous condition does not increase from the previous condition, and (3) exposure to such hazards does not change from the previous condition. If these conditions are met through the hazard analysis, then risk of the new condition shall be assumed to be proportional to the previous condition, and measured by calculation of the new system MTTHE.

6.2.2 Risk Assessment Basis

A full risk assessment shall address the safety risks affected when the product is deployed, modified, replaced, or enhanced. This includes risks associated with the *"previous condition"* which are eliminated as result of the change, new risks not present in the *"previous condition"*, and risks that are eliminated, added, changed, or whose severity or probability is affected versus the previous condition shall be included. A full risk assessment includes both qualitative and quantitative measures.

Safety levels shall be measured using competent risk assessment methods and shall 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 practices may be used with the written approval of the Alaska Railroad department or organization responsible for the system or product.

The risk assessment shall estimate the total risk associated with the implementation of the product. The principal focus is prevention of mishaps that result in fatalities, injuries, or asset damage. The risk assessment process shall include all aspects of the previous condition (e.g., the train control system) that is being replaced or improved by implementing the product (e.g., the processor-based signal or train control system). Exposure shall be expressed as total train miles/year. Severity shall identify the total cost, including fatalities, injuries, asset or property damage and other incidental costs. The relevant aspects include the method of operation, operating rules and practices, train crew, roadway worker, and dispatcher behaviors and training, and hardware and software on-board the train or roadway worker vehicle, or distributed along the wayside or at remote or office locations. Planned changes in the physical plant and operating conditions that are coincident with the introduction of the new safety-critical processor-based signal or train control system require the adjustment of the previous condition to reflect any associated impact on risk. An example would be increase train density or higher train speeds.

6.3 Risk Assessment Basis

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 shall be analyzed for the total change in risk, 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.)

The risk assessment shall be based primarily on the other work products that comprise the Product Safety Plan. Specifically, the following elements of the product safety process shall be used, as a minimum, to determine the risk of the product. Note that the listed items are thought to be significant inputs to the risk assessment, regardless of the assessment methodology used.

a. Standards for performing the risk assessment that are followed by the Vendor.

b. Results of Hazard Analyses, both of the product and of the product's interface with personnel and the railroad environment.

c. The quantitative basis for the evaluation of the risk, including the Vendor's statistical confidence level(s) and derivation thereof.

d. The results of the Safety Verification and Validation of the product.

e. The results of the safety testing of the complete product and any subsystems of the product.

f. The results of the Human Factors Analysis of the product, and identification of critical human faults than can directly lead to incidents or mishaps.

g. The operational safety assumptions contained in Part 19 – Safety Critical Assumptions and Feedback Operation, of the PSP.

6.4 Risk Assessment Assumptions and Sensitivity Analysis

Each assumption included in the risk assessment shall be thoroughly documented and reviewed for reasonableness. Sensitivity analysis shall be used to examine the expected impact that the assumption has on the risk assessment result if the assumption is subsequently proven to be incorrect.

6.5 Performance Risk Monitoring After Entering Operational Service [Rule §236.917(b)] and [Rule §236.907(a)(18)]

Alaska Railroad will monitor actual system performance after the safety-critical processor-based signal or 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 MTTHE or other measure than was stated in the Product Safety Plan for the mitigating function) shall be reported to the FRA and additionally as required by Rule §236.917(b).

This process shall encompass the requirement for monitoring of the system risks that relate to ongoing operation and maintenance. The Vendor shall comply with both Section 5.17 of this Railroad Safety Program Plan and with Rule §236.907(a)(18) in this regard. Alaska Railroad shall specify in contracts with the Vendor, such records that shall be kept by the Vendor during initial revenue service, throughout the warranty period, and while system is under maintenance contract. The Vendor shall promptly notify the Alaska Railroad the department or organization responsible for the system or product if the risk assessment has been negatively affected by the field experience.

The Alaska Railroad monitoring program will also identify the occurrence of hazards associated with the product that were not previously identified in the Product Safety Plan. Hazards that were not previously identified in the PSP shall be assumed to have a threshold level MTTHE of zero and shall be subject to the requirements of Rule §236.917(b).

Following the warranty period, during which the vendor will maintain records, ARRC will initiate a maintenance contract with the Vendor to keep and/or maintain the required records until the maintenance contract is terminated. When the maintenance contract with

the Vendor is terminated, ARRC will assume the responsibility for keeping and maintaining all relevant records.

During the warranty and maintenance period, the Vendor shall promptly notify the Alaska Railroad organization responsible for the system or product if the risk assessment has been negatively affected by the field experience.

7 PSP Review and Approval [§236.913]

7.1 Railroad Review and Approval of PSP

The Product Safety Plan (PSP) for each signal or train control system subject to the provision of 49 CFR §236 Part H shall be reviewed and approved by Alaska Railroad prior to submission to the Federal Railroad Administration.

The Product Safety Plan (PSP) for each active highway-rail grade crossing warning system subject to the provision of 49 CFR §236 Part H and 49 CFR §234.275 shall be reviewed and approved by Alaska Railroad prior to submission to the Federal Railroad Administration.

The suitability and readiness for submission of a Product Safety Plan (PSP) to the Federal Railroad Administration by Alaska Railroad shall be at the sole discretion of Alaska Railroad.

The Product Safety Plan review and approval process for each signal system, active highway-rail grade crossing warning system or train control system subject to the provisions of 49 CFR §236 Part H and/or 49 CFR §234.275 shall be defined by Alaska Railroad. The review and approval process will include participation by the Federal Railroad Administration, and may include participation by other joint facility rail carriers to facilitate final approval of the Product Safety Plan.

8 Implementation and Operation [§236.915]

8.1 Compliance with PSP and RSPP Requirements

Implementation of a new or novel safety-critical processor-based signal or train control system shall be in full compliance with all requirements in this Railroad Safety Program Plan and the approved Product Safety Plan prior to beginning operations. Evidence of compliance shall be accurately and completely documented and shall be established through review of documentary evidence, safety V&V testing, or other reviews or analyses necessary to establish full compliance with safety requirements.

Railroad operations after implementation of the system or product shall remain in full compliance with the operational design limits as specified in the Product Safety Plan and the regulations in 49 CFR §236.915 for safety-critical processor-based signal or train control system implementation and operation.

The Alaska Railroad department or organization responsible for the design development and/or deployment of a safety-critical processor-based system or product shall be responsible for ensuring that the Vendor for the system (subsystem or component) or product complies with the requirements of this Railroad Safety Program Plan and all applicable Federal Regulations.

8.2 Restrictions on Testing of Safety-critical Processor Based Signal and Train Control Components, System, or Subsystems

Procedures shall be established to ensure safe train movement and operations during testing of a new or novel safety-critical processor-based signal or train control system, subsystems or component. These procedures shall be integrated into standard testing and maintenance procedures and training programs for test and maintenance personnel to the satisfactions of Alaska Railroad and with the written approval of the Alaska Railroad department or organization responsible for the system or product.

8.3 System or Subsystem Failures

Failures of any safety-critical processor-based signal or train control system, subsystem or component shall be investigated, the cause determined and necessary adjustment, repair or replacement shall be promptly completed. Causes of failure shall be investigated and where necessary, resolution action taken to prevent or reduce the probability of recurrent failure. Safety of train movements and of roadway workers shall be ensured during the adjustment, repair or replacement process. The Alaska Railroad department or organization responsible for the system or product has the responsibility to investigate system, subsystem and/or component failures, and to take corrective action to mitigate the failure.

8.4 Informational Product Safety Plan Filing

New or novel safety-critical processor-based signal or train control systems, subsystems or components not requiring Federal Railroad Administration approval may be placed in revenue service 180 days after filing with FRA an informational filing for that product per 49 CFR §236.915(a)(1). Implementation of such new or novel products or systems shall be in full compliance with the requirements in this Railroad Safety Program Plan and the approved Product Safety Plan for the subject product or system. Evidence of compliance shall be accurately and completely documented and shall be established through review of documentary evidence, safety V&V testing or other reviews or analyses necessary to establish full compliance with safety requirements.

After implementation of the new or novel product, railroad operations shall remain in full compliance with the operation design limits as specified in the Product Safety Plan and the requirements contained in 49 CFR §236.915.

Except as stated in 49 CFR §236.915(a)(3), if Federal Railroad Administration approval is required for a safety-critical processor-based signal or train control system (subsystem or component) or product, Alaska Railroad shall not operate the system (subsystem or component) or product in revenue service until after the Associate Administrator for Safety has approved the petition for approval of the system or product pursuant to 49 CFR §236.

9 System Operations and Maintenance Manual [§236.919]

A combined[5] Operation and Maintenance Manual (OMM), herein after referred to as the Manual, shall be delivered to Alaska Railroad by the Vendor, consisting of all documents specified in the Product Safety Plan for installation, maintenance, repair, modification, inspection, and testing of the safety-critical processor-based signal or train control system. Alaska Railroad will properly catalog the contents of the Manual, and will maintain a copy of the Manual, in a format selected by Alaska Railroad, at all locations where needed to properly perform such tasks. The Manual shall be delivered in a mutually agreeable hard copy format, and in a mutually agreeable digital media. The Manual shall be available for inspection by the FRA.

Additionally, current and correct plans and layouts required for the proper maintenance, repair, inspection and testing of the system shall be delivered by the Vendor in hard copy format digital media and copies of these documents shall be maintained by Alaska Railroad where such products are deployed or maintained. Revision control for both hardware and software will be included.

Alaska Railroad configuration management control will ensure that the current hardware, software, and firmware revisions are identified and included in the Manual and plans where relevant. During the Vendor's involvement, the vendor shall also maintain proper configuration control per the approved Product Safety Plan.

Alaska Railroad requires that all safety-critical components be positively identified, handled, replaced and repaired per specific procedures described by the Vendor in the Manual. Such procedures are intended to preserve the safety characteristics of the system or product and components and shall be specified in the Product Safety Plan.

The Operations and Maintenance Manual (OMM) shall be based on the system-specific procedures specified in the Product Safety Plan and consistent with Alaska Railroad overall operating rules and practices. The Manual shall address the following activities associated with the product:

[5] Alaska Railroad and the Vendor shall be responsible for the production of a single comprehensive Operations Maintenance Manual when multiple vendors are involved in the development of a system or product.

- Installation and Deployment.
- Periodic maintenance and testing.
- Modification.
- Repair.
- Operation under normal and fallback modes.

10 Training and Qualification Program [§236.921, §236.923, §236.925, §236.927, and §236.929]

Alaska Railroad will establish and implement training and qualification programs that provide the knowledge and skill set required for basic job performance for those Alaska Railroad employees whose duties require interaction with the safety-critical processor-based signal or train control system. Alaska Railroad shall retain and maintain records identifying Alaska Railroad employees that are qualified.

The Product Safety Plan shall provide a description of the training required to ensure the safe installation, implementation, operation, maintenance, repair, inspection, testing and/or modification of the safety-critical processor-based signal or train control system for both normal and abnormal conditions. These programs shall address the minimum Alaska Railroad training and qualification requirements for workers whose duties include:

- Installing, inspecting, testing, maintaining, modifying, or repairing the safety-critical processor-based signal or train control system, subsystems, or components, including wayside or on-board equipment. This requirement shall apply to a safety-critical or vital central office system that is a component of the subject signal or train control system.
- Train dispatching operations within the safety-critical processor-based signal or train control system territory.
- Operating trains or serving as a train crew member in safety-critical processor-based signal or train control system territory.
- Activities on the roadway requiring knowledge and understanding of the safety-critical processor-based signal or train control system (e.g., Roadway Workers).
- Direct supervision of any of the above designated employees.

Alaska Railroad training programs shall address both initial training and continuing training and qualification programs necessary to maintain worker skills. Training program design, execution and record keeping shall be in accordance with the requirements specified in the related FRA regulations [§236.921, §236.923, §236.925, §236.927, and §236.929].

11 Human-Machine Interface [Part 236, Appendix E]

Because processor-based signal and train control systems involve human interaction with potentially complex functions that provide safety to the railroad, Alaska Railroad requires that the Vendor use ergonomic design criteria as specified in the development of the Human Machine Interface (HMI). The Vendor shall describe the proposed HMI features of the system for Alaska Railroad approval as part of the design documentation. Proper reference to the specific design documents shall be included in the Product Safety Plan for completeness.

Proper design of HMI will support vigilant attention by the operating personnel and encourage appropriate action where needed to assure safety of the railroad operation. HMI designers must be familiar with the safety-critical processor-based signal or train control system and its operating environment. The following shall be considered as requirements for the HMI of the Vendor system:

a. The system shall require regular operator interactions or shall alert the operator.

b. The system shall provide timely feedback in response to operator inputs or changing conditions, with an understandable explanation of the content of the feedback.

c. The system shall prompt operators for necessary input in advance of the time the input is needed.

d. The HMI shall provide consistent and predictable display of information and use consistent formats for obtaining necessary inputs from the operator.

e. The system shall arrange and integrate information to facilitate the operator's ability to respond correctly.

f. The system design shall use simple standardized formats that minimize time to respond to information presented.

g. The system shall minimize the information displayed to, at most, three independent functions.

h. The system shall provide automatically refreshable display that can supplement the operator's memory.

i. The system design shall optimize the location, size, color and movement of HMI controls used by the operator.