ALASKA RAILROAD CORPORATION
Railroad Safety Program Plan Rev 2
March 5, 2007

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	

Table of Contents

Section Title Page

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.

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 and a list of the applicable systems on the ARRC.

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 establishes definitive requirements for a Product Safety Plan (PSP) that will be prepared for implementation, operation, and maintenance of a processor-based signal and train control system on the ARRC.

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 Product Safety Plan (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.

- Section 5 presents requirements for the development of a PSP as defined in §236.907.

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
RSPP	Railroad Safety Program Plan
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	(Something like) 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. The latest revisions of each of these references shall apply.

A. Alaska Railroad Airbrake and Train Handling Rules, Effective May 7, 2006.

B. Alaska Railroad Corporation Timetable No 133. In Effect at 06:00 Sunday May 7, 2006.

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

D. Alaska Railroad Corporation Train Dispatcher Manual, Effective 0001, Monday May 29, 2006.

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

3 System Deployment

Deployment of the CAS processor-based signal and train control system will be on 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

ARRC Divisions using train control governed by this RSPP may include DTC and CTC operating rules and control methods.

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 Product Safety Plan 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 shall assume ultimate responsibility for the complete, correct and safe execution of all elements of this RSPP. A committee, including members of the ARRC safety organization, along with knowledgeable representatives of the ARRC product development organization, shall make recommendations to the ARRC Assistant Vice President of Operating Rules and Control Systems for his approval.

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 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.

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 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.

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.

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.

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.

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

The fail-safe processor-based signal and train control system will be implemented and managed using a comprehensive safety assurance process that addresses the life cycle of the system. This safety assurance process will be focused on identifying and resolving hazards associated with the system. 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 a set of 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 help 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 RSPP 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.

A copy of any non-published standards shall be included with the PSP.

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.

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 vendors 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 ARRC approval.

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

Formal 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 (CM) plan 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 compatible with ARRC requirements and existing methodology. The CM plan 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 and shall contain at least the minimum criteria to satisfy the requirements as mandated by regulatory statutes.

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.

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 supporting the vendor's PSP shall be available for review and audit by the ARRC and the ARRC's designee. The vendor must consider the following subsections 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 Divisions involved. This section of the PSP will also describe the maximum train volume, train frequency, operating speed, and other physical capacities as applicable, for which the system is designed.

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, and references to source documents supporting the action.
8. Notation of whether the hazard is OPEN (requiring further action) or CLOSED (resolution action(s) complete and approved by ARRC).

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 will be part of the final Hazard Log submission in the PSP.

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.

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.

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 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.

5.9 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) Acceptable standards for verification and validation are:

1. The standards employed for verification and/or validation of the processor-based signal and train control system are subject to this subpart must be sufficient to support achievement of the applicable requirements of this subpart
2. 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.
3. The standards identified in 236H Appendix C, paragraph c, subparagraph (3).
4. 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 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)]

The vendor, working with ARRC, shall document in the PSP the training requirements necessary for ARRC personnel to ensure safe operation of the processor-based signal and train control system. 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, on a test track, or on an operating line of the railroad.
- Safety validation testing of the proposed system, using production equipment, shall be performed where necessary on ARRC track prior to final acceptance to assure that all safety-critical functions and algorithms are implemented safely, especially those that are influenced by physical characteristics of the train and the railroad infrastructure.
- 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.

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)]

The PSP shall contain a complete description of all initial implementation testing procedures necessary to establish that safety-functional requirements are met and safety-critical hazards are appropriately mitigated.

The PSP shall contain descriptions of pre-implementation factory testing, field-testing procedures, 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 will 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 vendor shall provide the ARRC with the test plans and procedures developed per this requirement, and obtain approval of test plans 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.

This part of the PSP shall 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.

Part 9 of this PSP 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 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.

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.