

## 49 CFR

### Part 236—Rules, Standards, and Instructions Governing the Installation, Inspection, Maintenance, and Repair of Signal and Train Control Systems, Devices, and Appliances

#### General

#### 236.18

##### §236.18 Software management control plan.

(a) Within 6 months of June 6, 2005, each railroad shall develop and adopt a software management control plan for its signal and train control systems. A railroad commencing operations after June 6, 2005, shall adopt a software management control plan for its signal and train control systems prior to commencing operations.

(b) Within 30 months of the completion of the software management control plan, each railroad shall have fully implemented such plan.

(c) For purposes of this section, "software management control plan" means a plan designed to ensure that the proper and intended software version for each specific site and location is documented (mapped) and maintained through the life-cycle of the system. The plan must further describe how the proper software configuration is to be identified and confirmed in the event of replacement, modification, or disarrangement of any part of the system.

[70 FR 11052, March 07, 2005]

##### §236.110 Results of tests.

(a) Results of tests made in compliance with § 236.102 to 236.109, inclusive; 236.376 to 236.387, inclusive; 236.576; 236.577; 236.586 to 236.589, inclusive; and 236.917(a) must be recorded on preprinted forms provided by the railroad or by electronic means, subject to approval by the FRA Associate Administrator for Safety. These records must show the name of the railroad, place and date, equipment tested, results of tests, repairs, replacements, adjustments made, and condition in which the apparatus was left. Each record must be:

(1) Signed by the employee making the test, or electronically coded or identified by number of the automated test equipment (where applicable);

(2) Unless otherwise noted, filed in the office of a supervisory official having jurisdiction; and

(3) Available for inspection and replication by FRA and FRA-certified State inspectors.

(b) Results of tests made in compliance with § 236.587 must be retained for 92 days.

(c) Results of tests made in compliance with § 236.917(a) must be retained as follows:

(1) Results of tests that pertain to installation or modification must be retained for the life-cycle of the equipment tested and may be kept in any office designated by the railroad; and

(2) Results of periodic tests required for maintenance or repair of the equipment tested must be retained until the next record is filed but in no case less than one year.

(d) Results of all other tests listed in this section must be retained until the next record is filed but in no case less than one year.

(e) Electronic or automated tracking systems used to meet the requirements contained in paragraph (a) of this section must be capable of being reviewed and monitored by FRA at any time to ensure the integrity of the system. FRA's Associate Administrator for Safety may prohibit or revoke a railroad's authority to utilize an electronic or automated tracking system in lieu of preprinted forms if FRA finds that the electronic or automated tracking system is not properly secured, is inaccessible to FRA, FRA-certified State inspectors, or railroad employees requiring access to discharge their assigned duties, or fails to adequately track and monitor the equipment. The Associate Administrator for Safety will provide the affected railroad with a written statement of the basis for his or her decision prohibiting or revoking the railroad from utilizing an electronic or automated tracking system.

Amended: [53 FR 37313, Sept. 26, 1988; 70 FR 11052, March 07, 2005]

## Part 236 Subpart H

### **Subpart H—Standards for Processor-Based Signal and Train Control Systems**

§236.901	Purpose and scope.
§236.903	Definitions.
§236.905	Railroad Safety Program Plan (RSPP).
§236.907	Product Safety Plan (PSP).
§236.909	Minimum performance standard.
§236.911	Exclusions.
§236.913	Filing and approval of PSPs.
§236.915	Implementation and operation.
§236.917	Retention of records.
§236.919	Operations and Maintenance Manual.
§236.921	Training and qualification program, general.
§236.923	Task analysis and basic requirements.
§236.925	Training specific to control office personnel.

§236.927 Training specific to locomotive engineers and other operating personnel.  
§236.929 Training specific to roadway workers.  
Source: 70 FR 11052, March 07, 2005

§236.901 Purpose and scope.

(a) What is the purpose of this subpart? The purpose of this subpart is to promote the safe operation of processor-based signal and train control systems, subsystems, and components that are safety-critical products, as defined in § 236.903, and to facilitate the development of those products.

(b) What topics does it cover? This subpart prescribes minimum, performance-based safety standards for safety-critical products, including requirements to ensure that the development, installation, implementation, inspection, testing, operation, maintenance, repair, and modification of those products will achieve and maintain an acceptable level of safety. This subpart also prescribes standards to ensure that personnel working with safety-critical products receive appropriate training. Each railroad may prescribe additional or more stringent rules, and other special instructions, that are not inconsistent with this subpart.

(c) What other rules apply?

(1) This subpart does not exempt a railroad from compliance with the requirements of subparts A through G of this part, except to the extent a PSP explains to FRA Associate Administrator for Safety's satisfaction the following:

(i) How the objectives of any such requirements are met by the product;

(ii) Why the objectives of any such requirements are not relevant to the product; or

(iii) How the requirement is satisfied using alternative means. (See § 236.907(a)(14)).

(2) Products subject to this subpart are also subject to applicable requirements of parts 233, 234 and 235 of this chapter. See § 234.275 of this chapter with respect to use of this subpart to qualify certain products for use within highway-rail grade crossing warning systems.

(3) Information required to be submitted by this subpart that a submitter deems to be trade secrets, or commercial or financial information that is privileged or confidential under Exemption 4 of the Freedom of Information Act, 5 U.S.C. 552(b)(4), shall be so labeled in accordance with the provisions of § 209.11 of this chapter. FRA handles information so labeled in accordance with the provisions of § 209.11 of this chapter.

§236.903 Definitions.

As used in this subpart-

Associate Administrator for Safety means the Associate Administrator for Safety, FRA, or that person's delegate as designated in writing.

Component means an element, device, or appliance (including those whose nature is electrical, mechanical, hardware, or software) that is part of a system or subsystem.

Configuration management control plan means a plan designed to ensure that the proper and intended product configuration, including the hardware components and software version, is documented and maintained through the life-cycle of the products in use.

Employer means a railroad, or contractor to a railroad, that directly engages or compensates individuals to perform the duties specified in § 236.921(a).

Executive software means software common to all installations of a given product. It generally is used to schedule the execution of the site-specific application programs, run timers, read inputs, drive outputs, perform self-diagnostics, access and check memory, and monitor the execution of the application software to detect unsolicited changes in outputs.

FRA means the Federal Railroad Administration.

Full automatic operation means that mode of an automatic train control system capable of operating without external human influence, in which the locomotive engineer/operator may act as a passive system monitor, in addition to an active system controller.

Hazard means an existing or potential condition that can result in an accident.

High degree of confidence, as applied to the highest level of aggregation, means there exists credible safety analysis supporting the conclusion that the likelihood of the proposed condition associated with the new product being less safe than the previous condition is very small.

Human factors refers to a body of knowledge about human limitations, human abilities, and other human characteristics, such as behavior and motivation, that must be considered in product design.

Human-machine interface (HMI) means the interrelated set of controls and displays that allows humans to interact with the machine.

Initialization refers to the startup process when it is determined that a product has all required data input and the product is prepared to function as intended.

Mandatory directive has the meaning set forth in § 220.5 of this chapter.

Materials handling refers to explicit instructions for handling safety-critical components established to comply with procedures specified in the PSP.

Mean Time To Hazardous Event (MTTHE) means the average or expected time that a subsystem or component will operate prior to the occurrence of an unsafe failure.

New or next-generation train control system means a train control system using technologies not in use in revenue service at the time of PSP submission or without established histories of safe practice.

Petition for approval means a petition to FRA for approval to use a product on a railroad as described in its PSP. The petition for approval is to contain information that is relevant to determining the safety of the resulting system; relevant to determining compliance

with this part; and relevant to determining the safety of the product, including a complete copy of the product's PSP and supporting safety analysis.

Predefined change means any post-implementation modification to the use of a product that is provided for in the PSP (see § 236.907(b)).

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 (including the elements of any existing signal or train control system relevant to the review of the product).

Processor-based, as used in this subpart, means dependent on a digital processor for its proper functioning.

Product means a processor-based signal or train control system, subsystem, or component.

Product Safety Plan (or PSP) refers to a formal document which describes in detail all of the safety aspects of the product, including but not limited to procedures for its development, installation, implementation, operation, maintenance, repair, inspection, testing and modification, as well as analyses supporting its safety claims, as described in § 236.907.

Railroad Safety Program Plan (or RSPP) refers to a formal document which describes a railroad's strategy for addressing safety hazards associated with operation of products under this subpart and its program for execution of such strategy through the use of PSP requirements, as described in § 236.905.

Revision control means a chain of custody regimen designed to positively identify safety-critical components and spare equipment availability, including repair/replacement tracking in accordance with procedures outlined in the PSP.

Risk means the expected probability of occurrence for an individual accident event (probability) multiplied by the severity of the expected consequences associated with the accident (severity).

Risk assessment means the process of determining, either quantitatively or qualitatively, the measure of risk associated with use of the product under all intended operating conditions or the previous condition.

Safety-critical, as applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel or equipment, or both; or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist.

Subsystem means a defined portion of a system.

System refers to a signal or train control system and includes all subsystems and components thereof, as the context requires.

System Safety Precedence means the order of precedence in which methods used to eliminate or control identified hazards within a system are implemented.

Validation means 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."

Verification means 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."

**§236.905**      Railroad Safety Program Plan (RSPP).

(a) What is the purpose of an RSPP?

A railroad subject to this subpart shall develop an RSPP, subject to FRA approval, that serves as its principal safety document for all safety-critical products. The RSPP must establish the minimum PSP requirements that will govern the development and implementation of all products subject to this subpart, consistent with the provisions contained in § 236.907.

(b) What subject areas must the RSPP address?

The railroad's RSPP must address, at a minimum, the following subject areas:

(1) Requirements and concepts. The RSPP must require a description of the preliminary safety analysis, including:

(i) A complete description of methods used to evaluate a system's behavioral characteristics;

(ii) A complete description of risk assessment procedures;

(iii) The system safety precedence followed; and

(iv) The identification of the safety assessment process.

(2) *Design for verification and validation.* The RSPP must require the identification of verification and validation methods for the preliminary safety analysis, initial development process, and future incremental changes, including standards to be used in the verification and validation process, consistent with Appendix C to this part. The RSPP must require that references to any non-published standards be included in the PSP.

(3) *Design for human factors.* The RSPP must require a description of the process used during product development to identify human factors issues and develop design requirements which address those issues.

(4) *Configuration management control plan.* The RSPP must specify requirements for configuration management for all products to which this subpart applies.

(c) How are RSPP's approved?

(1) Each railroad shall submit a petition for approval of an RSPP in triplicate to the Associate Administrator for Safety, FRA, 1120 Vermont Avenue, NW., Mail Stop 25, Washington, DC 20590. The petition must contain a copy of the proposed RSPP, and the name, title, address, and telephone number of the railroad's primary contact person for review of the petition.

(2) Normally within 180 days of receipt of a petition for approval of an RSPP, FRA:

(i) Grants the petition, if FRA finds that the petition complies with applicable requirements of this subpart, attaching any special conditions to the approval of the petition as necessary to carry out the requirements of this subpart;

(ii) Denies the petition, setting forth reasons for denial; or

(iii) Requests additional information.

(3) If no action is taken on the petition within 180 days, the petition remains pending for decision. The petitioner is encouraged to contact FRA for information concerning its status.

(4) FRA may reopen consideration of any previously-approved petition for cause, providing reasons for such action.

(d) How are RSPP's modified?

(1) Railroads shall obtain FRA approval for any modification to their RSPP which affects a safety-critical requirement of a PSP. Other modifications do not require FRA approval.

(2) Petitions for FRA approval of RSPP modifications are subject to the same procedures as petitions for initial RSPP approval, as specified in paragraph (c) of this section. In addition, such petitions must identify the proposed modification(s) to be made, the reason for the modification(s), and the effect of the modification(s) on safety.

#### **§236.907**      Product Safety Plan (PSP).

(a) What must a PSP contain?

The PSP must include the following:

(1) A complete description of the product, including a list of all product components and their physical relationship in the subsystem or system;

(2) A description of the railroad operation or categories of operations on which the product is designed to be used, including train movement density, gross tonnage, passenger train movement density, hazardous materials volume, railroad operating rules, and operating speeds;

(3) An operational concepts document, including a complete description of the product functionality and information flows;

(4) A safety requirements document, including a list with complete descriptions of all functions which the product performs to enhance or preserve safety;

- (5) A document describing the manner in which product architecture satisfies safety requirements;
- (6) A hazard log consisting of a comprehensive description of all safety-relevant hazards to be addressed during the life cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence);
- (7) A risk assessment, as prescribed in § 236.909 and Appendix B to this part;
- (8) A hazard mitigation analysis, including a complete and comprehensive description of all hazards to be addressed in the system design and development, mitigation techniques used, and system safety precedence followed, as prescribed by the applicable RSPP;
- (9) A complete description of the safety assessment and verification and validation processes applied to the product and the results of these processes, describing how subject areas covered in Appendix C to this part are either: addressed directly, addressed using other safety criteria, or not applicable;
- (10) A complete description of the safety assurance concepts used in the product design, including an explanation of the design principles and assumptions;
- (11) A human factors analysis, including a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the product to enhance or preserve safety, and an analysis in accordance with Appendix E to this part or in accordance with other criteria if demonstrated to the satisfaction of the Associate Administrator for Safety to be equally suitable;
- (12) A complete description of the specific training of railroad and contractor employees and supervisors necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product;
- (13) A complete description of the specific procedures and test equipment necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations;
- (14) An analysis of the applicability of the requirements of subparts A through G of this part to the product that may no longer apply or are satisfied by the product using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled (see § 234.275 of this chapter and § 236.901(c));
- (15) A complete description of the necessary security measures for the product over its life-cycle;



(16) A complete description of each warning to be placed in the Operations and Maintenance Manual identified in § 236.919, and of all warning labels required to be placed on equipment as necessary to ensure safety;

(17) 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;

(18) A complete description of:

(i) 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, through use, or after maintenance (repair, replacement, adjustment) is performed; and

(ii) Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards (see § 236.917(e)(3));

(19) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and

(20) A complete description of all incremental and predefined changes (see paragraphs (b) and (c) of this section).

(b) What requirements apply to predefined changes?

(1) Predefined changes are not considered design modifications requiring an entirely new safety verification process, a revised PSP, and an informational filing or petition for approval in accordance with § 236.915. However, the risk assessment for the product must demonstrate that operation of the product, as modified by any predefined change, satisfies the minimum performance standard.

(2) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change. (Software changes involving safety functional requirements or safety critical hazard mitigation processes for components in use are also addressed in paragraph (c) of this section.)

(c) What requirements apply to other product changes?

(1) Incremental changes are planned product version changes described in the initial PSP where slightly different specifications are used to allow the gradual enhancement of the product's capabilities. Incremental changes shall require verification and validation to the extent the changes involve safety-critical functions.

(2) Changes classified as maintenance require validation.

(d) What are the responsibilities of the railroad and product supplier regarding communication of hazards?

(1) The PSP shall specify all contractual arrangements with hardware and software suppliers for immediate notification of any and all safety critical software upgrades, patches, or revisions for their processor-based system, sub-system, or component, and the reasons for such changes from the suppliers, whether or not the railroad has experienced a failure of that safety-critical system, sub-system, or component.

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

(3) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change, and that any such change can be audited.

(4) Product suppliers entering into contractual arrangements for product support described in a PSP must promptly report any safety-relevant failures and previously unidentified hazards to each railroad using the product.

**§236.909**      Minimum performance standard.

(a) What is the minimum performance standard for products covered by this subpart? The safety analysis included in the railroad's PSP must establish with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. The railroad shall determine, prior to filing its petition for approval or informational filing, that this standard has been met and shall make available the necessary analyses and documentation as provided in this subpart.

(b) How does FRA determine whether the PSP requirements for products covered by subpart H have been met?

With respect to any FRA review of a PSP, the Associate Administrator for Safety independently determines whether the railroad's safety case establishes with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. In evaluating the sufficiency of the railroad's case for the product, the Associate Administrator for Safety considers, as applicable, the factors pertinent to evaluation of risk assessments, listed in § 236.913(g)(2).

(c) What is the scope of a full risk assessment required by this section?

A full risk assessment performed under this subpart must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This

includes risks associated with the previous condition which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature (probability of occurrence or severity) is nonetheless affected by the change.

(d) What is an abbreviated risk assessment, and when may it be used?

(1) An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard if:

(i) No new hazards are introduced as a result of the change;

(ii) Severity of each hazard associated with the previous condition does not increase from the previous condition; and

(iii) Exposure to such hazards does not change from the previous condition.

(2) An abbreviated risk assessment supports the finding required by paragraph (a) of this section if it establishes that the resulting MTTHE for the proposed product is greater than or equal to the MTTHE for the system, component or method performing the same function in the previous condition. This determination must be supported by credible safety analysis sufficient to persuade the Associate Administrator for Safety that the likelihood of the new product's MTTHE being less than the MTTHE for the system, component, or method performing the same function in the previous condition is very small.

(3) Alternatively, an abbreviated risk assessment supports the finding required by paragraph (a) of this section if:

(i) The probability of failure for each hazard of the product is equal to or less the corresponding recommended Specific Quantitative Hazard Probability Ratings classified as more favorable than "undesirable" by AREMA Manual Part 17.3.5 (Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications), or-in the case of a hazard classified as undesirable-the Associate Administrator for Safety concurs that mitigation of the hazard within the framework of the electronic system is not practical and the railroad proposes reasonable steps to undertake other mitigation. The Director of the Federal Register approves the incorporation by reference of the entire AREMA Communications and Signal Manual, Volume 4, Section 17-Quality Principles (2005) in this section in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of the incorporated standard from American Railway Engineering and Maintenance of Way Association, 8201 Corporation Drive, Suite 1125, Landover, MD 20785-2230. You may inspect a copy of the incorporated standard at the Federal Railroad Administration, Docket Clerk, 1120 Vermont Ave., NW., Suite 7000, or at the National Archives and Records Administration (NARA). For information on the availability of this

material at NARA, call 202-741-6030, or go to <http://www.archives.gov/federal-register/code-of-federal-regulations/ibr-locations.html>;

(ii) The product is developed in accordance with:

(A) AREMA Manual Part 17.3.1 (Communications and Signal Manual of Recommended Practices, Recommended Safety Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications);

(B) AREMA Manual Part 17.3.3 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications);

(C) AREMA Manual Part 17.3.5 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications);

(D) Appendix C

(iii) Analysis supporting the PSP suggests no credible reason for believing that the product will be less safe than the previous condition.

(e) How are safety and risk measured for the full risk assessment?

Risk assessment techniques, including both qualitative and quantitative methods, are recognized as providing credible and useful results for purposes of this section if they apply the following principles:

(1) Safety levels must be measured using competent risk assessment methods and must be expressed as the total residual risk in the system over its expected life-cycle after implementation of all mitigating measures described in the PSP. Appendix B to this part provides criteria for acceptable risk assessment methods. Other methods may be acceptable if demonstrated to the satisfaction of the Associate Administrator for Safety to be equally suitable.

(2) For the previous condition and for the life-cycle of the product, risk levels must be expressed in units of consequences per unit of exposure.

(i) In all cases exposure must be expressed as total train miles traveled per year. Consequences must identify the total cost, including fatalities, injuries, property damage, and other incidental costs, such as potential consequences of hazardous materials involvement, resulting from preventable accidents associated with the function(s) performed by the system. A railroad may, as an alternative, use a risk metric in which consequences are measured strictly in terms of fatalities.

(ii) In those cases where there is passenger traffic, a second risk metric must be calculated, using passenger-miles traveled per year as the exposure, and total societal

costs of passenger injuries and fatalities, resulting from preventable accidents associated with the function(s) performed by the system, as the consequences.

(3) If the description of railroad operations for the product required by § 236.907(a)(2) involves changes to the physical or operating conditions on the railroad prior to or within the expected life cycle of the product subject to review under this subpart, the previous condition shall be adjusted to reflect the lower risk associated with systems needed to maintain safety and performance at higher speeds or traffic volumes. In particular, the previous condition must be adjusted for assumed implementation of systems necessary to support higher train speeds as specified in § 236.0, as well as other changes required to support projected increases in train operations. The following specific requirements apply:

(i) If the current method of operation would not be adequate under § 236.0 for the proposed operations, then the adjusted previous condition must include a system as required under § 236.0, applied as follows:

(A) The minimum system where a passenger train is operated at a speed of 60 or more miles per hour, or a freight train is operated at a speed of 50 or more miles per hour, shall be a traffic control system;

(B) The minimum system where a train is operated at a speed of 80 or more miles per hour, but not more than 110 miles per hour, shall be an automatic cab signal system with automatic train control; and

(C) The minimum system where a train is operated at a speed of more than 110 miles per hour shall be a system determined by the Associate Administrator for Safety to provide an equivalent level of safety to systems required or authorized by FRA for comparable operations.

(ii) If the current method of operation would be adequate under § 236.0 for the proposed operations, but the current system is not at least as safe as a traffic control system, then the adjusted previous condition must include a traffic control system in the event of any change that results in:

(A) An annual average daily train density of more than twelve trains per day; or

(B) An increase in the annual average daily density of passenger trains of more than four trains per day.

(iii) Paragraph (e)(3)(ii)(A) of this section shall apply in all situations where train volume will exceed more than 20 trains per day but shall not apply to situations where train volume will exceed 12 trains per day but not exceed 20 trains per day, if in its PSP the railroad makes a showing sufficient to establish, in the judgment of the Associate Administrator for Safety, that the current method of operation is adequate for a specified volume of traffic in excess of 12 trains per day, but not more than 20 trains per day,

without material delay in the movement of trains over the territory and without unreasonable expenditures to expedite those movements when compared with the expense of installing and maintaining a traffic control system.

(4) In the case review of a PSP that has been consolidated with a proceeding pursuant to part 235 of this subchapter (see § 236.911(b)), the base case shall be determined as follows:

(i) If FRA determines that discontinuance or modification of the system should be granted without regard to whether the product is installed on the territory, then the base case shall be the conditions that would obtain on the territory following the discontinuance or modification. Note: This is an instance in which the base case is posited as greater risk than the actual (unadjusted) previous condition because the railroad would have obtained relief from the requirement to maintain the existing signal or train control system even if no new product had been proffered.

(ii) If FRA determines that discontinuance or modification of the system should be denied without regard to whether the product is installed on the territory, then the base case shall remain the previous condition (unadjusted).

(iii) If, after consideration of the application and review of the PSP, FRA determines that neither paragraph (e)(4)(i) nor paragraph (e)(4)(ii) of this section should apply, FRA will establish a base case that is consistent with safety and in the public interest.

#### §236.911 Exclusions.

(a) Does this subpart apply to existing systems? The requirements of this subpart do not apply to products in service as of June 6, 2005. Railroads may continue to implement and use these products and components from these existing products.

(b) How will transition cases be handled?

Products designed in accordance with subparts A through G of this part which are not in service but are developed or are in the developmental stage prior to March 7, 2005, may be excluded upon notification to FRA by June 6, 2005, if placed in service by March 7, 2008. Railroads may continue to implement and use these products and components from these existing products. A railroad may at any time elect to have products that are excluded made subject to this subpart by submitting a PSP as prescribed in § 236.913 and otherwise complying with this subpart.

(c) How are office systems handled?

The requirements of this subpart do not apply to existing office systems and future deployments of existing office system technology. However, a subsystem or component of an office system must comply with the requirements of this subpart if it performs safety-critical functions within, or affects the safety performance of, a new or next-

generation train control system. For purposes of this section, "office system" means a centralized computer-aided train-dispatching system or centralized traffic control board.

(d) How are modifications to excluded products handled?

Changes or modifications to products otherwise excluded from the requirements of this subpart by this section are not excluded from the requirements of this subpart if they result in a degradation of safety or a material increase in safety-critical functionality.

(e) What other rules apply to excluded products?

Products excluded by this section from the requirements of this subpart remain subject to subparts A through G of this part as applicable.

§236.913 Filing and approval of PSPs.

(a) Under what circumstances must a PSP be prepared?

A PSP must be prepared for each product covered by this subpart. A joint PSP must be prepared when:

(1) The territory on which a product covered by this subpart is normally subject to joint operations, or is operated upon by more than one railroad; and

(2) The PSP involves a change in method of operation.

(b) Under what circumstances must a railroad submit a petition for approval for a PSP or PSP amendment, and when may a railroad submit an informational filing?

Depending on the nature of the proposed product or change, the railroad shall submit either an informational filing or a petition for approval. Submission of a petition for approval is required for PSPs or PSP amendments concerning installation of new or next-generation train control systems. All other actions that result in the creation of a PSP or PSP amendment require an informational filing and are handled according to the procedures outlined in paragraph (c) of this section. Applications for discontinuance and material modification of signal and train control systems remain governed by parts 235 and 211 of this chapter; and petitions subject to this section may be consolidated with any relevant application for administrative handling.

(c) What are the procedures for informational filings?

The following procedures apply to PSPs and PSP amendments which do not require submission of a petition for approval, but rather require an informational filing:

(1) Not less than 180 days prior to planned use of the product in revenue service as described in the PSP or PSP amendment, the railroad shall submit an informational filing to the Associate Administrator for Safety, FRA, 1120 Vermont Avenue, NW., Mail Stop 25, Washington, DC 20590. The informational filing must provide a summary description of the PSP or PSP amendment, including the intended use of the product, and specify the location where the documentation as described in § 236.917(a)(1) is maintained.

(2) Within 60 days of receipt of the informational filing, FRA:

(i) Acknowledges receipt of the filing;

(ii) Acknowledges receipt of the informational filing and requests further information; or

(iii) Acknowledges receipt of the filing and notifies the railroad, for good cause, that the filing will be considered as a petition for approval as set forth in paragraph (d) of this section, and requests such further information as may be required to initiate action on the petition for approval. Examples of good cause, any one of which is sufficient, include: the PSP describes a product with unique architectural concepts; the PSP describes a product that uses design or safety assurance concepts considered outside existing accepted practices (see Appendix C); and the PSP describes a locomotive-borne product that commingles safety-critical train control processing functions with locomotive operational functions. In addition, good cause includes any instance where the PSP or PSP amendment does not appear to support its safety claim of satisfaction of the performance standard, after FRA has requested further information as provided in paragraph (c)(2)(ii) of this section.

(d) What procedures apply to petitions for approval?

The following procedures apply to PSPs and PSP amendments which require submission of a petition for approval:

(1) Petitions for approval involving prior FRA consultation.

(i) The railroad may file a Notice of Product Development with the Associate Administrator for Safety not less than 30 days prior to the end of the system design review phase of product development and 180 days prior to planned implementation, inviting FRA to participate in the design review process and receive periodic briefings and updates as needed to follow the course of product development. At a minimum, the Notice of Product Development must contain a summary description of the product to be developed and a brief description of goals for improved safety.

(ii) Within 15 days of receipt of the Notice of Product Development, the Associate Administrator for Safety either acknowledges receipt or acknowledges receipt and requests more information.

(iii) If FRA concludes that the Notice of Product Development contains sufficient information, the Associate Administrator for Safety determines the extent and nature of the assessment and review necessary for final product approval. FRA may convene a technical consultation as necessary to discuss issues related to the design and planned development of the product.

(iv) Within 60 days of receiving the Notice of Product Development, the Associate Administrator for Safety provides a letter of preliminary review with detailed findings, including whether the design concepts of the proposed product comply with the



requirements of this subpart, whether design modifications are necessary to meet the requirements of this subpart, and the extent and nature of the safety analysis necessary to comply with this subpart.

(v) Not less than 60 days prior to use of the product in revenue service, the railroad shall file with the Associate Administrator for Safety a petition for final approval.

(vi) Within 30 days of receipt of the petition for final approval, the Associate Administrator for Safety either acknowledges receipt or acknowledges receipt and requests more information. Whenever possible, FRA acts on the petition for final approval within 60 days of its filing by either granting it or denying it. If FRA neither grants nor denies the petition for approval within 60 days, FRA advises the petitioner of the projected time for decision and conducts any further consultations or inquiries necessary to decide the matter.

(2) Other petitions for approval. The following procedures apply to petitions for approval of PSPs which do not involve prior FRA consultation as described in paragraph (d)(1) of this section.

(i) Not less than 180 days prior to use of a product in revenue service, the railroad shall file with the Associate Administrator for Safety a petition for approval.

(ii) Within 60 days of receipt of the petition for approval, FRA either acknowledges receipt, or acknowledges receipt and requests more information.

(iii) Whenever possible, considering the scope, complexity, and novelty of the product or change, FRA acts on the petition for approval within 180 days of its filing by either granting it or denying it. If FRA neither grants nor denies the petition for approval within 180 days, it remains pending, and FRA provides the petitioner with a statement of reasons why the petition has not yet been approved.

(e) What role do product users play in the process of safety review?

(1) FRA will publish in the Federal Register periodically a topic list including docket numbers for informational filings and a petition summary including docket numbers for petitions for approval.

(2) Interested parties may submit to FRA information and views pertinent to FRA's consideration of an informational filing or petition for approval. FRA considers comments to the extent practicable within the periods set forth in this section. In a proceeding consolidated with a proceeding under part 235 of this chapter, FRA considers all comments received.

(f) Is it necessary to complete field testing prior to filing the petition for approval? A railroad may file a petition for approval prior to completion of field testing of the product. The petition for approval should additionally include information sufficient for

FRA to arrange monitoring of the tests. The Associate Administrator for Safety may approve a petition for approval contingent upon successful completion of the test program contained in the PSP or hold the petition for approval pending completion of the tests.

(g) How are PSPs approved?

(1) The Associate Administrator for Safety grants approval of a PSP when:

(i) The petition for approval has been properly filed and contains the information required in § 236.907;

(ii) FRA has determined that the PSP complies with the railroad's approved RSPP and applicable requirements of this subpart; and

(iii) The risk assessment supporting the PSP demonstrates that the proposed product satisfies the minimum performance standard stated in § 236.909.

(2) The Associate Administrator for Safety considers the following applicable factors when evaluating the risk assessment:

(i) The extent to which recognized standards have been utilized in product design and in the relevant safety analysis;

(ii) The availability of quantitative data, including calculations of statistical confidence levels using accepted methods, associated with risk estimates;

(iii) The complexity of the product and the extent to which it will incorporate or deviate from design practices associated with previously established histories of safe operation;

(iv) The degree of rigor and precision associated with the safety analyses, including the comprehensiveness of the qualitative analyses, and the extent to which any quantitative results realistically reflect appropriate sensitivity cases;

(v) The extent to which validation of the product has included experiments and tests to identify uncovered faults in the operation of the product;

(vi) The extent to which identified faults are effectively addressed;

(vii) Whether the risk assessment for the previous condition was conducted using the same methodology as that for operation under the proposed condition; and

(viii) If an independent third-party assessment is required or is performed at the election of the supplier or railroad, the extent to which the results of the assessment are favorable.

(3) The Associate Administrator for Safety also considers when assessing PSPs the safety requirements for the product within the context of the proposed method of operations, including:

(i) The degree to which the product is relied upon as the primary safety system for train operations; and

(ii) The degree to which the product is overlaid upon and its operation is demonstrated to be independent of safety-relevant rules, practices and systems that will remain in place following the change under review.

(4) As necessary to ensure compliance with this subpart and with the RSPP, FRA may attach special conditions to the approval of the petition.

(5) Following the approval of a petition, FRA may reopen consideration of the petition for cause. Cause for reopening a petition includes such circumstances as a credible allegation of error or fraud, assumptions determined to be invalid as a result of in-service experience, or one or more unsafe events calling into question the safety analysis underlying the approval.

(h) Under what circumstances may a third-party assessment be required, and by whom may it be conducted?

(1) The PSP must be supported by an independent third party assessment of the product when FRA concludes it is necessary based upon consideration of the following factors:

(i) Those factors listed in paragraphs (g)(2)(i) through (g)(2)(vii) of this section;

(ii) The sufficiency of the assessment or audit previously conducted at the election of a supplier or railroad; and

(iii) Whether applicable requirements of subparts A through G of this part are satisfied.

(2) As used in this section, "independent third party" means a technically competent entity responsible to and compensated by the railroad (or an association on behalf of one or more railroads) that is independent of the supplier of the product. An entity that is owned or controlled by the supplier, that is under common ownership or control with the supplier, or that is otherwise involved in the development of the product is not considered "independent" within the meaning of this section. FRA may maintain a roster of recognized technically competent entities as a service to railroads selecting reviewers under this section; however, a railroad is not limited to entities currently listed on any such roster.

(3) The third-party assessment must, at a minimum, consist of the activities and result in production of documentation meeting the requirements of Appendix D to this part. However, when requiring an assessment pursuant to this section, FRA specifies any

requirements in Appendix D to this part which the agency has determined are not relevant to its concerns and, therefore, need not be included in the assessment. The railroad shall make the final assessment report available to FRA upon request.

(i) How may a PSP be amended?

A railroad may submit an amendment to a PSP at any time in the same manner as the initial PSP. Notwithstanding the otherwise applicable requirements found in this section and § 236.915, changes affecting the safety-critical functionality of a product may be made prior to the submission and approval of the PSP amendment as necessary in order to mitigate risk.

(j) How may field testing be conducted prior to PSP approval?

(1) Field testing of a product may be conducted prior to the approval of a PSP by the submission of an informational filing by a railroad. The FRA will arrange to monitor the tests based on the information provided in the filing, which must include:

(i) A complete description of the product;

(ii) An operational concepts document;

(iii) A complete description of the specific test procedures, including the measures that will be taken to protect trains and on-track equipment;

(iv) An analysis of the applicability of the requirements of subparts A through G of this part to the product that will not apply during testing;

(v) The date testing will begin;

(vi) The location of the testing; and

(vii) A description of any effect the testing will have on the current method of operation.

(2) FRA may impose such additional conditions on this testing as may be necessary for the safety of train operations. Exemptions from regulations other than those contained in this part must be requested through waiver procedures in part 211 of this chapter.

Amended: [70 FR 72385, Dec. 5, 2005]

**§236.915**      Implementation and operation.

(a) When may a product be placed or retained in service?

(1) Except as stated in paragraphs (a)(2) and (a)(3) of this section, a railroad may operate in revenue service any product 180 days after filing with FRA the informational filing for that product. The FRA filing date can be found in FRA's acknowledgment letter referred to in § 236.913(c)(2).

(2) Except as stated in paragraph (a)(3) of this section, if FRA approval is required for a product, the railroad shall not operate the product in revenue service until after the Associate Administrator for Safety has approved the petition for approval for that product pursuant to § 236.913.

(3) If after product implementation FRA elects, for cause, to treat the informational filing for the product as a petition for approval, the product may remain in use if otherwise consistent with the applicable law and regulations. FRA may impose special conditions for use of the product during the period of review for cause.

(b) How does the PSP relate to operation of the product? Each railroad shall comply with all provisions in the PSP for each product it uses and shall operate within the scope of initial operational assumptions and predefined changes identified by the PSP. Railroads may at any time submit an amended PSP according to the procedures outlined in § 236.913.

(c) What precautions must be taken prior to interference with the normal functioning of a product? The normal functioning of any safety-critical product must not be interfered with in testing or otherwise without first taking measures to provide for safe movement of trains, locomotives, roadway workers and on-track equipment that depend on normal functioning of such product.

(d) What actions must be taken immediately upon failure of a safety-critical component? When any safety-critical product component fails to perform its intended function, the cause must be determined and the faulty component adjusted, repaired, or replaced without undue delay. Until repair of such essential components are completed, a railroad shall take appropriate action as specified in the PSP. See also § § 236.907(d), 236.917(b).

**§ 236.917**      Retention of records.

(a) What life-cycle and maintenance records must be maintained?

(1) The railroad shall maintain at a designated office on the railroad:

(i) For the life-cycle of the product, adequate documentation to demonstrate that the PSP meets the safety requirements of the railroad's RSPP and applicable standards in this subpart, including the risk assessment; and

(ii) An Operations and Maintenance Manual, pursuant to § 236.919; and

(iii) Training records pursuant to § 236.923(b).

(2) Results of inspections and tests specified in the PSP must be recorded as prescribed in § 236.110.

(3) Contractors of the railroad shall maintain at a designated office training records pursuant to § 236.923(b).

(b) What actions must the railroad take in the event of occurrence of a safety-relevant hazard?

After the product is placed in service, the railroad shall maintain a database of all safety-relevant hazards as set forth in the PSP and those that had not been previously identified in the PSP. If the frequency of the safety-relevant hazards exceeds the threshold set forth in the PSP (see § 236.907(a)(6)), then the railroad shall:

(1) Report the inconsistency in writing (by mail, facsimile, e-mail, or hand delivery to the Director, Office of Safety Assurance and Compliance, FRA, 1120 Vermont Ave., NW., Mail Stop 25, Washington, DC 20590, within 15 days of discovery. Documents that are hand delivered must not be enclosed in an envelope;

(2) Take prompt countermeasures to reduce the frequency of the safety-relevant hazard(s) below the threshold set forth in the PSP; and

(3) Provide a final report to the FRA Director, Office of Safety Assurance and Compliance, on the results of the analysis and countermeasures taken to reduce the frequency of the safety-relevant hazard(s) below the threshold set forth in the PSP when the problem is resolved.

**§236.919**      Operations and Maintenance Manual.

(a) The railroad shall catalog and maintain all documents as specified in the PSP for the installation, maintenance, repair, modification, inspection, and testing of the product and have them in one Operations and Maintenance Manual, readily available to persons required to perform such tasks and for inspection by FRA and FRA-certified State inspectors.

(b) Plans required for proper maintenance, repair, inspection, and testing of safety-critical products must be adequate in detail and must be made available for inspection by FRA and FRA-certified State inspectors where such products are deployed or maintained. They must identify all software versions, revisions, and revision dates. Plans must be legible and correct.

(c) Hardware, software, and firmware revisions must be documented in the Operations and Maintenance Manual according to the railroad's configuration management control plan and any additional configuration/revision control measures specified in the PSP.

(d) Safety-critical components, including spare equipment, must be positively identified, handled, replaced, and repaired in accordance with the procedures specified in the PSP.

**§236.921**      Training and qualification program, general.

(a) When is training necessary and who must be trained?

Employers shall establish and implement training and qualification programs for products subject to this subpart. These programs must meet the minimum requirements set forth in the PSP and in § § 236.923 through 236.929 as appropriate, for the following personnel:

(1) Persons whose duties include installing, maintaining, repairing, modifying, inspecting, and testing safety-critical elements of the railroad's products, including central office, wayside, or onboard subsystems;

(2) Persons who dispatch train operations (issue or communicate any mandatory directive that is executed or enforced, or is intended to be executed or enforced, by a train control system subject to this subpart);

(3) Persons who operate trains or serve as a train or engine crew member subject to instruction and testing under part 217 of this chapter, on a train operating in territory where a train control system subject to this subpart is in use;

(4) Roadway workers whose duties require them to know and understand how a train control system affects their safety and how to avoid interfering with its proper functioning; and

(5) The direct supervisors of persons listed in paragraphs (a)(1) through (a)(4) of this section.

(b) What competencies are required?

The employer's program must provide training for persons who perform the functions described in paragraph (a) of this section to ensure that they have the necessary knowledge and skills to effectively complete their duties related to processor-based signal and train control equipment.

**§236.923**      Task analysis and basic requirements.

(a) How must training be structured and delivered?

As part of the program required by § 236.921, the employer shall, at a minimum:

(1) Identify the specific goals of the training program with regard to the target population (craft, experience level, scope of work, etc.), task(s), and desired success rate;

(2) Based on a formal task analysis, identify the installation, maintenance, repair, modification, inspection, testing, and operating tasks that must be performed on a railroad's products. This includes the development of failure scenarios and the actions expected under such scenarios;

(3) Develop written procedures for the performance of the tasks identified;

(4) Identify the additional knowledge, skills, and abilities above those required for basic job performance necessary to perform each task;

(5) Develop a training curriculum that includes classroom, simulator, computer-based, hands-on, or other formally structured training designed to impart the knowledge, skills, and abilities identified as necessary to perform each task;

(6) Prior to assignment of related tasks, require all persons mentioned in § 236.921(a) to successfully complete a training curriculum and pass an examination that covers the product and appropriate rules and tasks for which they are responsible (however, such persons may perform such tasks under the direct onsite supervision of a qualified person prior to completing such training and passing the examination);

(7) Require periodic refresher training at intervals specified in the PSP that includes classroom, simulator, computer-based, hands-on, or other formally structured training and testing, except with respect to basic skills for which proficiency is known to remain high as a result of frequent repetition of the task; and

(8) Conduct regular and periodic evaluations of the effectiveness of the training program specified in § 236.923(a)(1) verifying the adequacy of the training material and its validity with respect to current railroads products and operations.

(b) What training records are required?

Employers shall retain records which designate persons who are qualified under this section until new designations are recorded or for at least one year after such persons leave applicable service. These records shall be kept in a designated location and be available for inspection and replication by FRA and FRA-certified State inspectors.

**§236.925**      Training specific to control office personnel.

Any person responsible for issuing or communicating mandatory directives in territory where products are or will be in use must be trained in the following areas, as applicable:

(a) Instructions concerning the interface between the computer-aided dispatching system and the train control system, with respect to the safe movement of trains and other on-track equipment;

(b) Railroad operating rules applicable to the train control system, including provision for movement and protection of roadway workers, unequipped trains, trains with failed or cut-out train control onboard systems, and other on-track equipment; and

(c) Instructions concerning control of trains and other on-track equipment in case the train control system fails, including periodic practical exercises or simulations, and operational testing under part 217 of this chapter to ensure the continued capability of the personnel to provide for safe operations under the alternative method of operation.



**§236.927** Training specific to locomotive engineers and other operating personnel.

(a) What elements apply to operating personnel?

Training provided under this subpart for any locomotive engineer or other person who participates in the operation of a train in train control territory must be defined in the PSP and the following elements must be addressed:

(1) Familiarization with train control equipment onboard the locomotive and the functioning of that equipment as part of the system and in relation to other onboard systems under that person's control;

(2) Any actions required of the onboard personnel to enable, or enter data to, the system, such as consist data, and the role of that function in the safe operation of the train;

(3) Sequencing of interventions by the system, including pre-enforcement notification, enforcement notification, penalty application initiation and post-penalty application procedures;

(4) Railroad operating rules applicable to the train control system, including provisions for movement and protection of any unequipped trains, or trains with failed or cut-out train control onboard systems and other on-track equipment;

(5) Means to detect deviations from proper functioning of onboard train control equipment and instructions regarding the actions to be taken with respect to control of the train and notification of designated railroad personnel; and

(6) Information needed to prevent unintentional interference with the proper functioning of onboard train control equipment.

(b) How must locomotive engineer training be conducted?

Training required under this subpart for a locomotive engineer, together with required records, must be integrated into the program of training required by part 240 of this chapter.

(c) What requirements apply to full automatic operation?

The following special requirements apply in the event a train control system is used to effect full automatic operation of the train:

(1) The PSP must identify all safety hazards to be mitigated by the locomotive engineer.

(2) The PSP must address and describe the training required with provisions for the maintenance of skills proficiency. As a minimum, the training program must:

(i) As described in § 236.923(a)(2), develop failure scenarios which incorporate the safety hazards identified in the PSP, including the return of train operations to a fully manual mode;

(ii) Provide training, consistent with § 236.923(a), for safe train operations under all failure scenarios and identified safety hazards that affect train operations;

(iii) Provide training, consistent with § 236.923(a), for safe train operations under manual control; and

(iv) Consistent with § 236.923(a), ensure maintenance of manual train operating skills by requiring manual starting and stopping of the train for an appropriate number of trips and by one or more of the following methods:

(A) Manual operation of a train for a 4-hour work period;

(B) Simulated manual operation of a train for a minimum of 4 hours in a Type I simulator as required; or

(C) Other means as determined following consultation between the railroad and designated representatives of the affected employees and approved by the FRA. The PSP must designate the appropriate frequency when manual operation, starting, and stopping must be conducted, and the appropriate frequency of simulated manual operation.

**§236.929**      Training specific to roadway workers.

(a) How is training for roadway workers to be coordinated with part 214?

Training required under this subpart for a roadway worker must be integrated into the program of instruction required under part 214, subpart C of this chapter ("Roadway Worker Protection"), consistent with task analysis requirements of § 236.923. This training must provide instruction for roadway workers who provide protection for themselves or roadway work groups.

(b) What subject areas must roadway worker training include?

(1) Instruction for roadway workers must ensure an understanding of the role of processor-based signal and train control equipment in establishing protection for roadway workers and their equipment.

(2) Instruction for roadway workers must ensure recognition of processor-based signal and train control equipment on the wayside and an understanding of how to avoid interference with its proper functioning.

(3) Instructions concerning the recognition of system failures and the provision of alternative methods of on-track safety in case the train control system fails, including periodic practical exercises or simulations and operational testing under part 217 of this chapter to ensure the continued capability of roadway workers to be free from the danger of being struck by a moving train or other on-track equipment.

## Appendix B to Part 236—Risk Assessment Criteria

The safety-critical performance of each product for which risk assessment is required under this part must be assessed in accordance with the following criteria or other criteria if demonstrated to the Associate Administrator for Safety to be equally suitable:

(a) How are risk metrics to be expressed? The risk metric for the proposed product must describe with a high degree of confidence the accumulated risk of a train system that operates over a life-cycle of 25 years or greater. Each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis, and the risk value selected must be demonstrated to have a high degree of confidence.

(b) How does the risk assessment handle interaction risks for interconnected subsystems/components? The safety-critical assessment of each product must include all of its interconnected subsystems and components and, where applicable, the interaction between such subsystems.

(c) How is the previous condition computed? Each subsystem or component of the previous condition must be analyzed with a Mean Time To Hazardous Event (MTTHE) as specified subject to a high degree of confidence.

(d) What major risk characteristics must be included when relevant to assessment? Each risk calculation must consider the total signaling and train control system and method of operation, as subjected to a list of hazards to be mitigated by the signaling and train control system. The methodology requirements must include the following major characteristics, when they are relevant to the product being considered:

- (1) Track plan infrastructure;
- (2) Total number of trains and movement density;
- (3) Train movement operational rules, as enforced by the dispatcher and train crew behaviors;
- (4) Wayside subsystems and components; and
- (5) Onboard subsystems and components.

(e) What other relevant parameters must be determined for the subsystems and components? The failure modes of each subsystem or component, or both, must be determined for the integrated hardware/software (where applicable) as a function of the Mean Time To Failure (MTTF) failure restoration rates, and the integrated hardware/software coverage of all processor-based subsystems or components, or both. Train operating and movement rules, along with components that are layered in order to enhance safety-critical behavior, must also be considered.

(f) How are processor-based subsystems/components assessed?

- (1) An MTTHE value must be calculated for each processor-based subsystem or component, or both, indicating the safety-critical behavior of the integrated

hardware/software subsystem or component, or both. The human factor impact must be included in the assessment, whenever applicable, to provide an integrated MTTHE value. The MTTHE calculation must consider the rates of failures caused by permanent, transient, and intermittent faults accounting for the fault coverage of the integrated hardware/software subsystem or component, phased-interval maintenance, and restoration of the detected failures.

(2) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The compliance process must be demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to have a high degree of confidence.

(g) How are non-processor-based subsystems/components assessed?

(1) The safety-critical behavior of all non-processor-based components, which are part of a processor-based system or subsystem, must be quantified with an MTTHE metric. The MTTHE assessment methodology must consider failures caused by permanent, transient, and intermittent faults, phase-interval maintenance and restoration of failures and the effect of fault coverage of each non-processor-based subsystem or component.

(2) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The non-processor-based quantification compliance must be demonstrated to have a high degree of confidence.

(h) What assumptions must be documented?

(1) The railroad shall document any assumptions regarding the reliability or availability of mechanical, electric, or electronic components. Such assumptions must include MTTF projections, as well as Mean Time To Repair (MTTR) projections, unless the risk assessment specifically explains why these assumptions are not relevant to the risk assessment. The railroad shall document these assumptions in such a form as to permit later automated comparisons with in-service experience (e.g., a spreadsheet).

(2) The railroad shall document any assumptions regarding human performance. The documentation shall be in such a form as to facilitate later comparisons with in-service experience.

(3) The railroad shall document any assumptions regarding software defects. These assumptions shall be in a form which permits the railroad to project the likelihood of detecting an in-service software defect. These assumptions shall be documented in such a form as to permit later automated comparisons with in-service experience.

(4) The railroad shall document all of the identified safety-critical fault paths. The documentation shall be in such a form as to facilitate later comparisons with in-service faults.

[70 FR 11052, March 07, 2005]

## Appendix C to Part 236—Safety Assurance Criteria and Processes

(a) What is the purpose of this appendix?

This appendix seeks to promote full disclosure of safety risk to facilitate minimizing or eliminating elements of risk where practicable by providing minimum criteria and processes for safety analyses conducted in support of PSPs. The analysis required by this appendix is intended to minimize the probability of failure to an acceptable level, helping to optimize the safety of the product within the limitations of the available engineering science, cost, and other constraints. FRA uses the criteria and processes set forth in this appendix to evaluate analyses, assumptions, and conclusions provided in RSPP and PSP documents. An analysis performed under this appendix must:

- (1) Address each area of paragraph (b) of this appendix, explaining how such objectives are addressed or why they are not relevant, and
- (2) Employ a validation and verification process pursuant to paragraph (c) of this appendix.

(b) What categories of safety elements must be addressed?

The designer shall address each of the following safety considerations when designing and demonstrating the safety of products covered by subpart H of this part. In the event that any of these 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 (including all hardware and software) must demonstrate safe operation with no hardware failures under normal anticipated operating conditions with proper inputs and within the expected range of environmental conditions. All safety-critical functions must be performed properly under these normal conditions. Absence of specific operator actions or procedures will not prevent the system from operating safely. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

(2) Systematic failure. It must be shown how the product is designed to mitigate or eliminate unsafe systematic failures—those conditions 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 the software specification, design or coding phases, or both; 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.

(i) The product must be shown to operate safely under conditions of random hardware failure. This includes single as well as multiple hardware failures, particularly in instances where one or more failures could occur, remain undetected (latent) and react in

combination with a subsequent failure at a later time to cause an unsafe operating situation. In instances involving a latent failure, a subsequent failure is similar to there being a single failure. In the event of a transient failure, and if so designed, the system should restart itself if it is safe to do so. Frequency of attempted restarts must be considered in the hazard analysis required by § 236.907(a)(8).

(ii) There shall be no single point failures in the product that can result in hazards categorized as unacceptable or undesirable. Occurrence of credible single point failures that can result in hazards must be detected and the product must achieve a known safe state before falsely activating any physical appliance.

(iii) 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 product must achieve a known safe state before falsely activating any physical appliance.

(4) Common Mode failure. Another concern of multiple failure involves common mode failures in which two or more subsystems or components intended to compensate one another to perform the same function all fail by the same mode and result in unsafe conditions. This is of particular concern in instances in which two or more elements (hardware or software, or both) are used in combination to ensure safety. If a common mode failure exists, then any analysis performed under this appendix cannot rely on the assumption that failures are independent. Examples include: the use of redundancy in which two or more elements perform a given function in parallel and when one (hardware or software) element checks/monitors another element (of hardware or software) to help ensure its safe operation. Common mode failure relates to independence, which must be ensured in these instances. When dealing with the effects of hardware failure, the designer shall address the effects of the failure not only on other hardware, but also on the execution of the software, since hardware failures can greatly affect how the software operates.

(5) External influences. The product must be shown to operate safely when subjected to different external influences, including:

(i) Electrical influences such as power supply anomalies/transients, abnormal/improper input conditions (e.g., outside of normal range inputs relative to amplitude and frequency, unusual combinations of inputs) including those related to a human operator, and others such as electromagnetic interference or electrostatic discharges, or both;

(ii) Mechanical influences such as vibration and shock; and

(iii) Climatic conditions such as temperature and humidity.

(6) Modifications. Safety must be ensured following modifications to the hardware or software, or both. All or some of the concerns identified in this paragraph may be applicable depending upon the nature and extent of the modifications.

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

(8) Closed Loop Principle. The product design must require positive action to be taken in a prescribed manner to either begin product operation or continue product operation.

(9) Human Factors Engineering: The product design must sufficiently incorporate human factors engineering that is appropriate to the complexity of the product; the educational, mental, and physical capabilities of the intended operators and maintainers; the degree of required human interaction with the component; and the environment in which the product will be used.

(c) What standards are acceptable for verification and validation?

(1) The standards employed for verification or validation, or both, of products subject to this subpart must be sufficient to support achievement of the applicable requirements of subpart H of this part.

(2) U.S. Department of Defense Military Standard (MIL-STD) 882C, "System Safety Program Requirements" (January 19, 1993), is recognized as providing appropriate risk analysis processes for incorporation into verification and validation standards.

(3) The following standards designed for application to processor-based signal and train control systems are recognized as acceptable with respect to applicable elements of safety analysis required by subpart H of this part. The latest versions of the standards listed below should be used unless otherwise provided.

(i) IEEE 1483-2000, Standard for the Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control.

(ii) CENELEC Standards as follows:

(A) EN50126: 1999, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(B) EN50128 (May 2001), Railway Applications: Software for Railway Control and Protection Systems;

(C) EN50129: 2003, Railway Applications: Communications, Signaling, and Processing Systems-Safety Related Electronic Systems for Signaling; and

(D) EN50155:2001/A1:2002, Railway Applications: Electronic Equipment Used in Rolling Stock.

(iii) ATCS Specification 140, Recommended Practices for Safety and Systems Assurance.

(iv) ATCS Specification 130, Software Quality Assurance.

(v) AAR-AREMA 2005 Communications and Signal Manual of Recommended Practices, Part 17.

(vi) Safety of High Speed Ground Transportation Systems. Analytical Methodology for Safety Validation of Computer Controlled Subsystems. Volume II: Development of a Safety Validation Methodology. Final Report September 1995. Author: Jonathan F. Luedeke, Battelle. DOT/FRA/ORD-95/10.2.

(vii) IEC 61508 (International Electrotechnical Commission), Functional Safety of Electrical/Electronic/Programmable/Electronic Safety (E/E/P/ES) Related Systems, Parts 1-7 as follows:

(A) IEC 61508-1 (1998-12) Part 1: General requirements and IEC 61508-1 Corr. (1999-05) Corrigendum 1-Part 1:General Requirements.

(B) IEC 61508-2 (2000-05) Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

(C) IEC 61508-3 (1998-12) Part 3: Software requirements and IEC 61508-3 Corr.1(1999-04) Corrigendum 1-Part3: Software requirements.

(D) IEC 61508-4 (1998-12) Part 4: Definitions and abbreviations and IEC 61508-4 Corr.1(1999-04) Corrigendum 1-Part 4: Definitions and abbreviations.

(E) IEC 61508-5 (1998-12) Part 5: Examples of methods for the determination of safety integrity levels and IEC 61508-5 Corr.1 (1999-04) Corrigendum 1 Part 5: Examples of methods for determination of safety integrity levels.

(F) IEC 61508-6 (2000-04) Part 6: Guidelines on the applications of IEC 61508-2 and -3.

(G) IEC 61508-7 (2000-03) Part 7: Overview of techniques and measures.

(4) Use of unpublished standards, including proprietary standards, is authorized to the extent that such standards are shown to achieve the requirements of this part. However, any such standards shall be available for inspection and replication by FRA and for public examination in any public proceeding before the FRA to which they are relevant.

[70 FR 11052, March 07, 2005]

#### **Appendix D to Part 236—Independent Review of Verification and Validation**

(a) What is the purpose of this appendix?

This appendix provides minimum requirements for independent third-party assessment of product safety verification and validation pursuant to subpart H of this part. The goal of this assessment is to provide an independent evaluation of the product manufacturer's utilization of safety design practices during the product's development and testing phases, as required by the applicable railroad's RSPP, the product PSP, the requirements of subpart H of this part, and any other previously agreed-upon controlling documents or standards.

(b) What general requirements apply to the conduct of third party assessments?

(1) The supplier may request advice and assistance of the reviewer concerning the actions identified in paragraphs (c) through (g) of this appendix. However, the reviewer should not engage in design efforts, in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the product.

(2) The supplier shall provide the reviewer access to any and all documentation that the reviewer requests and attendance at any design review or walkthrough that the reviewer determines as necessary to complete and accomplish the third party assessment. The reviewer may be accompanied by representatives of FRA as necessary, in FRA's judgment, for FRA to monitor the assessment.

(c) What must be done at the preliminary level?

The reviewer shall evaluate with respect to safety and comment on the adequacy of the processes which the supplier applies to the design and development of the product. At a minimum, the reviewer shall compare the supplier processes with acceptable methodology and employ any other such tests or comparisons if they have been agreed to previously with FRA. Based on these analyses, the reviewer shall identify and document



any significant safety vulnerabilities which are not adequately mitigated by the supplier's (or user's) processes. Finally, the reviewer shall evaluate the adequacy of the railroad's RSPP, the PSP, and any other documents pertinent to the product being assessed.

(d) What must be done at the functional level?

(1) The reviewer shall analyze the Preliminary Hazard Analysis (PHA) for comprehensiveness and compliance with the railroad's RSPP.

(2) The reviewer shall analyze all Fault Tree Analyses (FTA), Failure Mode and Effects Criticality Analysis (FMECA), and other hazard analyses for completeness, correctness, and compliance with the railroad's RSPP.

(e) What must be done at the implementation level?

The reviewer shall randomly select various safety-critical software modules for audit to verify whether the requirements of the RSPP were followed. The number of modules audited must be determined as a representative number sufficient to provide confidence that all unaudited modules were developed in compliance with the RSPP.

(f) What must be done at closure?

(1) The reviewer shall evaluate and comment on the plan for installation and test procedures of the product for revenue service.

(2) The reviewer shall prepare a final report of the assessment. The report shall be submitted to the railroad prior to the commencement of installation testing and contain at least the following information:

(i) Reviewer's evaluation of the adequacy of the PSP, including the supplier's MTTF and risk estimates for the product, and the supplier's confidence interval in these estimates;

(ii) Product vulnerabilities which the reviewer felt were not adequately mitigated, including the method by which the railroad would assure product safety in the event of a hardware or software failure (i.e., how does the railroad assure that all potentially hazardous failure modes are identified?) and the method by which the railroad addresses comprehensiveness of the product design for the requirements of the operations it will govern (i.e., how does the railroad assure that all potentially hazardous operating circumstances are identified? Who records any deficiencies identified in the design process? Who tracks the correction of these deficiencies and confirms that they are corrected?);

(iii) A clear statement of position for all parties involved for each product vulnerability cited by the reviewer;

(iv) Identification of any documentation or information sought by the reviewer that was denied, incomplete, or inadequate;

(v) A listing of each RSPP procedure or process which was not properly followed;

(vi) Identification of the software verification and validation procedures for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(vii) Methods employed by the product manufacturer to develop safety-critical software, such as use of structured language, code checks, modularity, or other similar generally acceptable techniques; and

(viii) Method by which the supplier or railroad addresses comprehensiveness of the product design which considers the safety elements listed in paragraph (b) of appendix C to this part.

[70 FR 11052, March 07, 2005]