

(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 though 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: