AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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

Executive software means software common to all installations of a given electronic 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.

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.

Loosely coupled means an attribute of systems, referring to an approach to designing interfaces across systems, subsystems, or components to reduce the interdependencies between them—in particular, reducing the risk that changes within one system, subsystem, or component will create unanticipated changes within other system, subsystem, or component.

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

Product means any safety critical electronic locomotive control system, subsystem, or component, not including safety critical processor based signal and train control systems, whose functions are directly related to safe movement and stopping of the train as well as the associated man-machine interfaces irrespective of the location of the control system, subsystem, or component.

Revision control means a chain of custody regimen designed to positively identify safety-critical components and spare equipment availability, including repair/replacement tracking.

Safety Analysis refers to a formal set of documentation 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.

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 any electronic locomotive control system and includes all subsystems and components thereof, as the context requires.

Test facility means a track that is not part of the general railroad system of transportation and is being used exclusively for the purpose of testing equipment and has all of its public grade crossings protected.

Tightly Coupled means an attribute of systems, referring to an approach to designing interfaces across systems, subsystems, or components to maximize the interdependencies between them. In particular, increasing the risk that changes within one system, subsystem, or component will create unanticipated changes within other system, subsystem, or component.

[77 FR 21348, Apr. 9, 2012, as amended at 77 FR 75057, Dec. 19, 2012]

§ 229.307 Safety analysis.

(a) A railroad shall develop a Safety Analysis (SA) for each product subject to this subpart prior to the initial use of such product on their railroad.

(b) The SA shall:

(1) establish and document the minimum requirements that will govern the development and implementation of all products subject to this subpart, and be based on good engineering practice and should be consistent with the guidance contained in appendix F of this part in order to establish that a product's safety-critical functions will operate with a high degree of confidence in a fail-safe manner;

(2) Include procedures for immediate repair of safety-critical functions; and

(3) Be made available to FRA upon request.

(c) Each railroad shall comply with the SA requirements and procedures related to the development, implementation, and repair of a product subject to this subpart.

§ 229.309 Safety-critical changes and failures.

(a) Whenever a planned safety-critical design change is made to a product that is in use by a railroad and subject to this subpart, the railroad shall:

(1) Notify FRA's Associate Administrator for Safety of the design changes made by the product supplier;

(2) Ensure that the SA is updated as required;

(3) Conduct all safety-critical changes in a manner that allows the change to be audited;

(4) Specify all contractual arrangements with suppliers and private equipment owners for notification of any and all electronic safety-critical changes as well as safety-critical failures in the suppliers and private equipment owners' system, subsystem, or components, and the reasons for that change or failure from the suppliers or equipment owners, whether or not the railroad has experienced a failure of that safety critical system, sub-system, or component;

(5) Specify the railroad's procedures for action upon receipt of notification of a safety-critical change or failure of an electronic system, sub-system, or component, and until the upgrade or revision has been installed; and

(6) Identify all 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.

(b) Product suppliers and private equipment owners shall report any safety-critical changes and previously unidentified hazards to each railroad using the product or equipment.

(c) Private equipment owners shall establish configuration/revision control measures for control of safety-critical changes and identification of previously unidentified hazards.

§ 229.311 Review of SAs.

(a) Prior to the initial planned use of a product subject to this subpart, a railroad shall inform the Associate Administrator for Safety/Chief Safety Officer, FRA, 1200 New Jersey Avenue SE., Mail Stop 25, Washington, DC 20590 of the intent to place this product in service. The notification shall provide a description of the product, and identify the location where the complete SA documentation described in § 229.307, the testing records contained in § 229.313, and the training and qualification program described in § 229.319 is maintained.

(b) FRA may review or audit the SA within 60 days of receipt of the notification or anytime after the product is placed in use. If FRA has not notified the railroad of its intent to review or audit the SA within the 60-day period, the railroad may assume that FRA does not intend to review or audit, and place the product in use. FRA reserves the right, however, to conduct a review or audit at a later date.

(c) A railroad shall maintain and make available to FRA upon request all railroad or vendor documentation used to demonstrate that the product meets the safety requirements of the SA for the life-cycle of the product.

(d) After a product is placed in service, the railroad shall maintain a database of all safety-relevant hazards encountered with the product. The database shall include all hazards identified in the SA and those that had not been previously identified in the SA. If the frequency of the safety-relevant hazards exceeds the threshold set forth in the SA, then the railroad shall:

(1) Report the inconsistency by mail, facsimile, email, or hand delivery to the Director, Office of Safety Assurance and Compliance, FRA, 1200 New Jersey Ave. SE., Mail Stop 25, Washington, DC 20590, within 15 days of discovery;

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

(3) Provide a final report to FRA's Director, Office of Safety Assurance and Compliance, on the results of the analysis and countermeasures taken to