§ 236.1023 Errors and malfunctions.

(a) Each railroad implementing a PTC system on its property shall establish and continually update a PTC Product Vendor List (PTCPVL) that includes all vendors and suppliers of each PTC system, subsystem, component, and associated product, and process in use system-wide. The PTCPVL shall be made available to FRA upon request.

(b)(1) The railroad shall specify within its PTCSSP all contractual arrangements with hardware and software suppliers or vendors for immediate notification between the parties of any and all safety-critical software failures, upgrades, patches, or revisions, as well as any hardware repairs, replacements, or modifications for their PTC system, subsystems, or components.

(b)(2) A vendor or supplier, on receipt of a report of any safety-critical failure to their product, shall promptly notify all other railroads that are using that product, whether or not the other railroads have experienced the reported failure of that safety-critical system, subsystem, or component.

(3) The notification from a supplier to any railroad shall include explanation from the supplier of the reasons for such notification, the circumstances associated with the failure, and any recommended mitigation actions to be taken pending determination of the root cause and final corrective actions.

(c) The railroad shall:

(1) Specify the railroad’s process and procedures in its PTCSSP for action upon their receipt of notification of safety-critical failure, as well as receipt of a safety-critical upgrade, patch, revision, repair, replacement, or modification.

(2) Identify configuration/revision control measures in its PTCSSP that are designed to ensure the safety-functional requirements and the safety-critical hazard mitigation processes are not compromised as a result of any change and that such a change can be audited.

(d) The railroad shall provide to the applicable vendor or supplier the railroad’s procedures for action upon notification of a safety-critical failure, upgrade, patch, or revision for the PTC system, subsystem, component, product, or process, and actions to be taken until the faulty system, subsystem, or component has been adjusted, repaired, or replaced.

(e) After the product is placed in service, the railroad shall maintain a database of all safety-relevant hazards as set forth in the PTCSSP and those that had not previously been identified in the PTCSSP. If the frequency of the safety-relevant hazard exceeds the thresholds set forth in the PTCSSP, or has not been previously identified in the appropriate risk analysis, the railroad shall:

(1) Notify the applicable vendor or supplier and FRA of the failure, malfunction, or defective condition that decreased or eliminated the safety functionality;

(2) Keep the applicable vendor or supplier and FRA apprised on a continual basis of the status of any and all subsequent failures; and

(3) Take prompt counter measures to reduce or eliminate the frequency of the safety-relevant hazards below the threshold identified in the PTCSSP.

(f) Each notification to FRA required by this section shall:

(1) Be made within 15 days after the vendor, supplier, or railroad discovers the failure, malfunction, or defective condition. However, a report that is due on a Saturday or a Sunday may be delivered on the following Monday and one that is due on a holiday may be delivered on the next business day;

(2) Be transmitted in a manner and form acceptable to the Associate Administrator and by the most expedient method available; and

(3) Include as much available and applicable information as possible, including:

(i) PTC system name and model;

(ii) Identification of the part, component, or system involved, including the part number as applicable;
§ 236.1025

(iii) Nature of the failure, malfunctions, or defective condition;

(iv) Mitigation taken to ensure the safety of train operation, railroad employees, and the public; and

(v) The estimated time to correct the failure.

(4) In the event that all information required by paragraph (f)(3) of this section is not immediately available, the non-available information shall be forwarded to the Associate Administrator as soon as practicable in supplemental reports.

(g) Whenever any investigation of an accident or service difficulty report shows that a PTC system or product is unsafe because of a manufacturing or design defect, the railroad and its vendor or supplier shall, upon request of the Associate Administrator, report to the Associate Administrator the results of its investigation and any action taken or proposed to correct that defect.

(h) PTC system and product suppliers and vendors shall:

(1) Promptly report any safety-relevant failures or defective conditions, previously unidentified hazards, and recommended mitigation actions in their PTC system, subsystem, or component to each railroad using the product; and

(2) Notify FRA of any safety-relevant failure, defective condition, or previously unidentified hazard discovered by the vendor or supplier and the identity of each affected and notified railroad.

(i) The requirements of this section do not apply to failures, malfunctions, or defective conditions that:

(1) Are caused by improper maintenance or improper usage; or

(2) Have been previously identified to the FRA, vendor or supplier, and applicable user railroads.

(j) When any safety-critical PTC system, subsystem, or component fails to perform its intended function, the cause shall be determined and the faulty product adjusted, repaired, or replaced without undue delay. Until corrective action is completed, a railroad shall take appropriate action to ensure safety and reliability as specified within its PTCSP.

(k) Any railroad experiencing a failure of a system resulting in a more favorable aspect than intended or other condition hazardous to the movement of a train shall comply with the reporting requirements, including the making of a telephonic report of an accident or incident involving such failure, under part 233 of this chapter. Filing of one or more reports under part 233 of this chapter does not exempt a railroad, vendor, or supplier from the reporting requirements contained in this section.

§ 236.1025 [Reserved]

§ 236.1027 PTC system exclusions.

(a) The requirements of this subpart apply to each office automation system that performs safety-critical functions within, or affects the safety performance of, the PTC system. For purposes of this section, “office automation system” means any centralized or distributed computer-based system that directly or indirectly controls the active movement of trains in a rail network.

(b) Changes or modifications to PTC systems otherwise excluded from the requirements of this subpart by this section do not exclude those PTC systems from the requirements of this subpart if the changes or modifications result in a degradation of safety or a material decrease in safety-critical functionality.

(c) Primary train control systems cannot be integrated with locomotive electronic systems unless the complete integrated systems:

(1) Have been shown to be designed on fail-safe principles;

(2) Have demonstrated to operate in a fail-safe mode;

(3) Have a manual fail-safe fallback and override to allow the locomotive to be brought to a safe stop in the event of any loss of electronic control; and

(4) Are included in the approved and applicable PTCDP and PTCSP.

(d) PTC systems excluded by this section from the requirements of this subpart remain subject to subparts A through H of this part as applicable.