(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.

Subpart I—Positive Train Control Systems

SOURCE: 75 FR 2699, Jan. 15, 2010, unless otherwise noted.

§ 236.1001 Purpose and scope.

(a) This subpart prescribes minimum, performance-based safety standards for PTC systems required by 49 U.S.C. 20157, this subpart, or an FRA order, including requirements to ensure that the development, functionality, architecture, installation, implementation, inspection, testing, operation, maintenance, repair, and modification of those PTC systems will achieve and maintain an acceptable level of safety. This subpart also prescribes standards to ensure that personnel working with, and affected by, safety-critical PTC system related products receive appropriate training and testing.

(b) Each railroad may prescribe additional or more stringent rules, and other special instructions, that are not inconsistent with this subpart.

(c) This subpart does not exempt a railroad from compliance with any requirement of subparts A through H of this part or parts 233, 234, and 235 of this chapter, unless:

(1) It is otherwise explicitly excepted by this subpart; or

(2) The applicable PTCSP, as defined under § 236.1003 and approved by FRA under § 236.1015, provides for such an exception per § 236.1013.

§ 236.1003 Definitions.

(a) Definitions contained in subparts G and H of this part apply equally to this subpart.

(b) The following definitions apply to terms used only in this subpart unless otherwise stated:

After-arrival mandatory directive means an authority to occupy a track which is issued to a train that is not effective and not to be acted upon until after the arrival and passing of a train, or trains, specifically identified in the authority.

Associate Administrator means the FRA Associate Administrator for Railroad Safety/Chief Safety Officer.

Class I railroad means a railroad which in the last year for which revenues were reported exceeded the

threshold established under regulations of the Surface Transportation Board (49 CFR part 1201.1–1 (2008)).

Cleartext means the un-encrypted text in its original, human readable, form. It is the input of an encryption or encipher process, and the output of an decryption or decipher process.

Controlling locomotive means *Locomotive, controlling,* as defined in § 232.5 of this chapter.

Host railroad means a railroad that has effective operating control over a segment of track.

Interoperability means the ability of a controlling locomotive to communicate with and respond to the PTC railroad's positive train control system, including uninterrupted movements over property boundaries.

Limited operations means operations on main line track that have limited or no freight operations and are approved to be excluded from this subpart's PTC system implementation and operation requirements in accordance with § 236.1019(c);

Main line means, except as provided in § 236.1019 or where all trains are limited to restricted speed within a yard or terminal area or on auxiliary or industry tracks, a segment or route of railroad tracks:

(1) Of a Class I railroad, as documented in current timetables filed by the Class I railroad with the FRA under § 217.7 of this title, over which 5,000,000 or more gross tons of railroad traffic is transported annually; or

(2) Used for regularly scheduled intercity or commuter rail passenger service, as defined in 49 U.S.C. 24102, or both. Tourist, scenic, historic, or excursion operations as defined in part 238 of this chapter are not considered intercity or commuter passenger service for purposes of this part.

Main line track exclusion addendum (''MTEA'') means the document submitted under §§ 236.1011 and 236.1019 requesting to designate track as other than main line.

Medium speed means, *Speed, medium,* as defined in subpart G of this part.

NPI means a Notice of Product Intent (''NPI'') as further described in § 236.1013.

PIH materials means materials poisonous by inhalation, as defined in §§ 171.8, 173.115, and 173.132 of this title.

PTC means positive train control as further described in § 236.1005.

PTCDP means a PTC Development Plan as further described in § 236.1013.

PTCIP means a PTC Implementation Plan as required under 49 U.S.C. 20157 and further described in § 236.1011.

PTCPVL means a PTC Product Vendor List as further described in § 236.1023.

PTCSP means a PTC Safety Plan as further described in § 236.1015.

PTC railroad means each Class I railroad and each entity providing regularly scheduled intercity or commuter rail passenger transportation required to implement or operate a PTC system.

PTC System Certification means certification as required under 49 U.S.C. 20157 and further described in §§ 236.1009 and 236.1015.

Request for Amendment (''RFA'') means a request for an amendment of a plan or system made by a PTC railroad in accordance with § 236.1021.

Request for Expedited Certification (''REC'') means, as further described in § 236.1031, a request by a railroad to receive expedited consideration for PTC System Certification.

Restricted speed means, *Speed, restricted,* as defined in subpart G of this part.

Safe State means a system state that, when the system fails, cannot cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment.

Segment of track means any part of the railroad where a train operates.

Temporal separation means that passenger and freight operations do not operate on any segment of shared track during the same period and as further defined under § 236.1019 and the process or processes in place to assure that result.

Tenant railroad means a railroad, other than a host railroad, operating on track upon which a PTC system is required.

Track segment means segment of track.

Type Approval means a number assigned to a particular PTC system indicating FRA agreement that the PTC system could fulfill the requirements of this subpart.

Train means one or more locomotives, coupled with or without cars.

[75 FR 2699, Jan. 15, 2010, as amended at 77 FR 28305, May 14, 2012; 79 FR 49716, Aug. 22, 2014]

§ 236.1005 Requirements for Positive Train Control systems.

(a) *PTC system requirements.* Each PTC system required to be installed under this subpart shall:

(1) Reliably and functionally prevent:

(i) Train-to-train collisions—including collisions between trains operating over rail-to-rail at-grade crossings in accordance with the following risk-based table or alternative arrangements providing an equivalent level of safety as specified in an FRA approved PTCSP:

Crossing type	Max. speed	Protection required
(A) Interlocking—one or more PTC routes intersecting with one or more non-PTC routes.	≤40 miles per hour	Interlocking signal arrangement in accordance with the requirements of subparts A–G of this part and PTC enforced stop on PTC routes.
(B) Interlocking—one or more PTC routes intersecting with one or more non-PTC routes.	>40 miles per hour	Interlocking signal arrangement in accordance with the requirements of subparts A–G of this part, PTC enforced stop on all PTC routes, and either the use of other than full PTC technology that provides positive stop enforcement or a split-point derail incorporated into the signal system accompanied by 20 miles per hour maximum allowable speed on the approach of any intersecting non-PTC route.
(C) Interlocking—all PTC routes intersecting.	Any speed	Interlocking signal arrangements in accordance with the requirements of subparts A–G of this part, and PTC enforced stop on all routes.

(ii) Overspeed derailments, including derailments related to railroad civil engineering speed restrictions, slow orders, and excessive speeds over switches and through turnouts;

(iii) Incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge, as applicable and in accordance with part 214 of this chapter; and

(iv) The movement of a train through a main line switch in the improper position as further described in paragraph (e) of this section.

(2) Include safety-critical integration of all authorities and indications of a wayside or cab signal system, or other similar appliance, method, device, or system of equivalent safety, in a manner by which the PTC system shall provide associated warning and enforcement to the extent, and except as, described and justified in the FRA approved PTCDP or PTCSP, as applicable;

(3) As applicable, perform the additional functions specified in this subpart;

(4) Provide an appropriate warning or enforcement when:

(i) A derail or switch protecting access to the main line required by § 236.1007, or otherwise provided for in the applicable PTCSP, is not in its derailing or protecting position, respectively;

(ii) A mandatory directive is issued associated with a highway-rail grade crossing warning system malfunction as required by §§ 234.105, 234.106, or 234.107;

(iii) An after-arrival mandatory directive has been issued and the train or trains to be waited on has not yet passed the location of the receiving train;

(iv) Any movable bridge within the route ahead is not in a position to allow permissive indication for a train movement pursuant to § 236.312; and

(v) A hazard detector integrated into the PTC system that is required by paragraph (c) of this section, or otherwise provided for in the applicable PTCSP, detects an unsafe condition or transmits an alarm; and

(5) Limit the speed of passenger and freight trains to 59 miles per hour and 49 miles per hour, respectively, in areas without broken rail detection or equivalent safeguards.

(b) *PTC system installation*—(1) *Lines required to be equipped.* Except as otherwise provided in this subpart, each Class I railroad and each railroad providing or hosting intercity or commuter passenger service shall progressively equip its lines as provided in its approved PTCIP such that a PTC system certified under §236.1015 is installed and operated by the host railroad on each:

(i) Main line over which is transported any quantity of material poisonous by inhalation (PIH), including anhydrous ammonia, as defined in §§171.8, 173.115 and 173.132 of this title;

(ii) Main line used for regularly provided intercity or commuter passenger service, except as provided in §236.1019; and

(iii) Additional line of railroad as required by the applicable FRA approved PTCIP, this subpart, or an FRA order requiring installation of a PTC system by that date.

(2) *Initial baseline identification of lines.* For the purposes of paragraph (b)(1)(i) of this section, the baseline information necessary to determine whether a Class I railroad's track segment shall be equipped with a PTC system shall be determined and reported as follows:

(i) The traffic density threshold of 5 million gross tons shall be based upon calendar year 2008 gross tonnage, except to the extent that traffic may fall below 5 million gross tons for two consecutive calendar years and a PTCIP or an RFA reflecting this change is filed and approved under paragraph (b)(4) of this section and, if applicable, §236.1021.

(ii) The presence or absence of any quantity of PIH hazardous materials shall be determined by whether one or more cars containing such product(s) was transported over the track segment in calendar year 2008 or prior to the filing of the PTCIP, except to the extent that the PTCIP or RFA justifies, under paragraph (b)(4) of this section, removal of the subject track segment from the PTCIP listing of lines to be equipped.

(3) *Addition of track segments.* To the extent increases in freight rail traffic occur subsequent to calendar year 2008 that might affect the requirement to install a PTC system on any line not yet equipped, the railroad shall seek to amend its PTCIP by promptly filing an RFA in accordance with §236.1021. The following criteria apply:

(i) If rail traffic exceeds 5 million gross tons in any year after 2008, the tonnage shall be calculated for the preceding two calendar years and if the total tonnage for those two calendar years exceeds 10 million gross tons, a PTCIP or its amendment is required.

(ii) If PIH traffic is carried on a track segment as a result of a request for rail service or rerouting warranted under part 172 of this title, and if the line carries in excess of 5 million gross tons of rail traffic as determined under this paragraph, a PTCIP or its amendment is required. This does not apply when temporary rerouting is authorized in accordance with paragraph (g) of this section.

(iii) Once a railroad is notified by FRA that its RFA filed in accordance with this paragraph has been approved, the railroad shall equip the line with the applicable PTC system by December 31, 2015, or within 24 months, whichever is later.

(4) *Exclusion or removal of track segments from PTC baseline*—(i) *Routing changes.* In a PTCIP or an RFA, a railroad may request review of the requirement to install PTC on a track segment where a PTC system is otherwise required by this section, but has not yet been installed, based upon changes in rail traffic such as reductions in total traffic volume to a level below 5 million gross tons annually, cessation of passenger service or the approval of an MTEA, or the cessation of PIH materials traffic. Any such request shall be accompanied by estimated traffic projections for the next 5 years (e.g., as a result of planned rerouting, coordinations, or location of new business on the line).

(ii) FRA will approve the exclusion requested pursuant to paragraph (b)(4)(i) of this section if the railroad

establishes that, as of December 31, 2015:

(A) No passenger service will be present on the involved track segment or the passenger service will be subject to an MTEA approved in accordance with 49 CFR 236.1019; and

(B) No PIH traffic will be present on the involved track segment or the gross tonnage on the involved track segment will decline to below 5 million gross tons annually as computed over a 2-year period.

(iii) *Freight lines with de minimis risk not used for regularly provided intercity or commuter rail passenger service.* (A) In a PTCIP or an RFA, a railroad may request review of the requirement to install a PTC system on a track segment where a PTC system is otherwise required by this section, but has not yet been installed, based upon the presence of a minimal quantity of PIH materials traffic. Any such request shall be accompanied by estimated traffic projections for the next 5 years (e.g., as a result of planned rerouting, coordination, or location of new business on the line). Where the request involves prior or planned rerouting of PIH materials traffic, the railroad must provide the information and analysis identified in paragraph (b)(4)(i) of this section. The submission shall also include a full description of potential safety hazards on the segment of track and fully describe train operations over the line. This paragraph does not apply to line segments used for commuter rail or intercity rail passenger service.

(B) Absent special circumstances related to specific hazards presented by operations on the line segment, FRA will approve a request for relief under this paragraph for a rail line segment that meets all of the following criteria:

(*1*) That carries less than 15 million gross tons annually;

(*2*) That does not have a heavy grade as ''heavy grade'' is defined in §232.407 of this chapter for any train operating over the track segment;

(*3*) Where the railroad adopts and complies with an operating rule requiring the crew of any train approaching working limits established under part 214 of this chapter to notify the roadway worker in charge of the train's approach at least 2 miles in advance of the working limits or, if the train crew does not have advance knowledge of the working limits, as soon as practical;

(*4*) That carries fewer than 100 cars containing PIH materials per year, excluding those cars containing only a residue, as defined in §171.8 of this title, of PIH materials;

(*5*) That carries 2 or fewer trains per day carrying any quantity of PIH materials;

(*6*) Where trains carrying any quantity of PIH materials operate at speeds not to exceed 40 miles per hour; and

(*7*) Where any train transporting a car containing any quantity of PIH materials is operated with a vacant block ahead of and behind the train.

(C) FRA may, in its discretion, approve other track segments not used for regularly provided intercity or commuter passenger service that have posed an equivalent or lesser level of risk of a PTC-preventable accident or PIH materials release as those track segments covered by paragraph (b)(4)(iii)(B) of this section, where such other track segments are similar to those covered by paragraph (b)(4)(iii)(B) of this section.

(D) Failure to submit sufficient information will result in the denial of any request under this paragraph (b)(4)(ii). If the request is granted, on and after the date the line would have otherwise been required to be equipped under the schedule contained in the PTCIP and approved by FRA, operations on the line shall be conducted in accordance with any conditions attached to the grant, including implementation of proposed mitigations as applicable.

(5) *Line sales.* FRA does not approve removal of a line from the PTCIP exclusively based upon a representation that a track segment will be abandoned or sold to another railroad. In the event a track segment is approved for abandonment or transfer by the Surface Transportation Board, FRA will review at the request of the transferring and acquiring railroads whether the requirement to install PTC on the line should be removed given all of the circumstances, including expected traffic and hazardous materials levels, reservation of trackage or haulage rights

by the transferring railroad, routing analysis under part 172 of this chapter, commercial and real property arrangements affecting the transferring and acquiring railroads post-transfer, and such other factors as may be relevant to continue safe operations on the line. If FRA denies the request, the acquiring railroad shall install the PTC system on the schedule provided in the transferring railroad's PTCIP, without regard to whether it is a Class I railroad.

(6) *New rail passenger service.* No new intercity or commuter rail passenger service shall commence after December 31, 2020, until a PTC system certified under this subpart has been installed and made operative.

(7) *Implementation deadlines.* (i) Each railroad must complete full implementation of its PTC system by December 31, 2018.

(ii) A railroad is excepted from paragraph (b)(7)(i) of this section and must complete full implementation of its PTC system by December 31, 2020, or the date specified in its approved alternative schedule and sequence, whichever is earlier, only if the railroad:

(A) Installs all PTC hardware and acquires all spectrum necessary to implement its PTC system by December 31, 2018;

(B) Submits an alternative schedule and sequence providing for implementation of positive train control system as soon as practicable, but not later than December 31, 2020;

(C) Notifies the Associate Administrator in writing that it is prepared for review of its alternative schedule and sequence under 49 U.S.C. 20157(a)(3)(B); and

(D) Receives FRA approval of its alternative schedule and sequence.

(iii) If a railroad meets the criteria in paragraph (b)(7)(ii) of this section, the railroad must adhere to its approved alternative schedule and sequence and any of its subsequently approved amendments or required modifications.

(c) *Hazard detectors.* (1) All hazard detectors integrated into a signal or train control system on or after October 16, 2008, shall be integrated into PTC systems required by this subpart; and their warnings shall be appropriately and timely enforced as described in the applicable PTCSP.

(2) The applicable PTCSP must provide for receipt and presentation to the locomotive engineer and other train crew members of warnings from any additional hazard detectors using the PTC data network, onboard displays, and audible alerts. If the PTCSP so provides, the action to be taken by the system and by the crew members shall be specified.

(3) The PTCDP (as applicable) and PTCSP for any new service described in §236.1007 to be conducted above 90 miles per hour shall include a hazard analysis describing the hazards relevant to the specific route(s) in question (e.g., potential for track obstruction due to events such as falling rock or undermining of the track structure due to high water or displacement of a bridge over navigable waters), the basis for decisions concerning hazard detectors provided, and the manner in which such additional hazard detectors will be interfaced with the PTC system.

(d) *Event recorders.* (1) Each lead locomotive, as defined in part 229, of a train equipped and operating with a PTC system required by this subpart must be equipped with an operative event recorder, which shall:

(i) Record safety-critical train control data routed to the locomotive engineer's display that the engineer is required to comply with;

(ii) Specifically include text messages conveying mandatory directives, maximum authorized speeds, PTC system brake warnings, PTC system brake enforcements, and the state of the PTC system (e.g., cut in, cut out, active, or failed); and

(iii) Include examples of how the captured data will be displayed during playback along with the format, content, and data retention duration requirements specified in the PTCSP submitted and approved pursuant to this paragraph. If such train control data can be calibrated against other data required by this part, it may, at the election of the railroad, be retained in a separate memory module.

(2) Each lead locomotive, as defined in part 229, manufactured and in service after October 1, 2009, that is

equipped and operating with a PTC system required by this subpart, shall be equipped with an event recorder memory module meeting the crash hardening requirements of § 229.135 of this chapter.

(3) Nothing in this subpart excepts compliance with any of the event recorder requirements contained in § 229.135 of this chapter.

(e) *Switch position.* The following requirements apply with respect to determining proper switch position under this section. When a main line switch position is unknown or improperly aligned for a train's route in advance of the train's movement, the PTC system will provide warning of the condition associated with the following enforcement:

(1) A PTC system shall enforce restricted speed over any switch:

(i) Where train movements are made with the benefit of the indications of a wayside or cab signal system or other similar appliance, method, device, or system of equivalent safety proposed to FRA and approved by the Associate Administrator in accordance with this part; and

(ii) Where wayside or cab signal system or other similar appliance, method, device, or system of equivalent safety, requires the train to be operated at restricted speed.

(2) A PTC system shall enforce a positive stop short of any main line switch, and any switch on a siding where the allowable speed is in excess of 20 miles per hour, if movement of the train over the switch:

(i) Is made without the benefit of the indications of a wayside or cab signal system or other similar appliance, method, device, or system of equivalent safety proposed to FRA and approved by the Associate Administrator in accordance with this part; or

(ii) Would create an unacceptable risk. Unacceptable risk includes conditions when traversing the switch, even at low speeds, could result in direct conflict with the movement of another train (including a hand-operated crossover between main tracks, a hand-operated crossover between a main track and an adjoining siding or auxiliary track, or a hand-operated switch providing access to another subdivision or branch line, etc.).

(3) A PTC system required by this subpart shall be designed, installed, and maintained to perform the switch position detection and enforcement described in paragraphs (e)(1) and (e)(2) of this section, except as provided for and justified in the applicable, FRA approved PTCDP or PTCSP.

(4) The control circuit or electronic equivalent for all movement authorities over any switches, movable-point frogs, or derails shall be selected through circuit controller or functionally equivalent device operated directly by the switch points, derail, or by switch locking mechanism, or through relay or electronic device controlled by such circuit controller or functionally equivalent device, for each switch, movable-point frog, or derail in the route governed. Circuits or electronic equivalent shall be arranged so that any movement authorities less restrictive than those prescribed in paragraphs (e)(1) and (e)(2) of this section can only be provided when each switch, movable-point frog, or derail in the route governed is in proper position, and shall be in accordance with subparts A through G of this part, unless it is otherwise provided in a PTCSP approved under this subpart.

(f) *Train-to-train collision.* A PTC system shall be considered to be configured to prevent train-to-train collisions within the meaning of paragraph (a) of this section if trains are required to be operated at restricted speed and if the onboard PTC equipment enforces the upper limits of the railroad's restricted speed rule (15 or 20 miles per hour). This application applies to:

(1) Operating conditions under which trains are required by signal indication or operating rule to:

(i) Stop before continuing; or

(ii) Reduce speed to restricted speed and continue at restricted speed until encountering a more favorable indication or as provided by operating rule.

(2) Operation of trains within the limits of a joint mandatory directive.

(g) *Temporary rerouting.* A train equipped with a PTC system as required by this subpart may be temporarily rerouted onto a track not equipped with a PTC system and a

train not equipped with a PTC system may be temporarily rerouted onto a track equipped with a PTC system as required by this subpart in the following circumstances:

(1) *Emergencies.* In the event of an emergency—including conditions such as derailment, flood, fire, tornado, hurricane, earthquake, or other similar circumstance outside of the railroad's control—that would prevent usage of the regularly used track if:

(i) The rerouting is applicable only until the emergency condition ceases to exist and for no more than 14 consecutive calendar days, unless otherwise extended by approval of the Associate Administrator;

(ii) The railroad provides written or telephonic notification to the applicable Regional Administrator of the information listed in paragraph (i) of this section within one business day of the beginning of the rerouting made in accordance with this paragraph; and

(iii) The conditions contained in paragraph (j) of this section are followed.

(2) *Planned maintenance.* In the event of planned maintenance that would prevent usage of the regularly used track if:

(i) The maintenance period does not exceed 30 days;

(ii) A request is filed with the applicable Regional Administrator in accordance with paragraph (i) of this section no less than 10 business days prior to the planned rerouting; and

(iii) The conditions contained in paragraph (j) of this section are followed.

(h) *Rerouting requests.* (1) For the purposes of paragraph (g)(2) of this section, the rerouting request shall be self-executing unless the applicable Regional Administrator responds with a notice disapproving of the rerouting or providing instructions to allow rerouting. Such instructions may include providing additional information to the Regional Administrator or Associate Administrator prior to the commencement of rerouting. Once the Regional Administrator responds with a notice under this paragraph, no rerouting may occur until the Regional Administrator or Associate Administrator provides his or her approval.

(2) In the event the temporary rerouting described in paragraph (g)(2) of this section is to exceed 30 consecutive calendar days:

(i) The railroad shall provide a request in accordance with paragraphs (i) and (j) of this section with the Associate Administrator no less than 10 business days prior to the planned rerouting; and

(ii) The rerouting shall not commence until receipt of approval from the Associate Administrator.

(i) *Content of rerouting request.* Each notice or request referenced in paragraph (g) and (h) of this section must indicate:

(1) The dates that such temporary rerouting will occur;

(2) The number and types of trains that will be rerouted;

(3) The location of the affected tracks; and

(4) A description of the necessity for the temporary rerouting.

(j) *Rerouting conditions.* Rerouting of operations under paragraph (g) of this section may occur under the following conditions:

(1) Where a train not equipped with a PTC system is rerouted onto a track equipped with a PTC system, or a train not equipped with a PTC system that is compatible and functionally responsive to the PTC system utilized on the line to which the train is being rerouted, the train shall be operated in accordance with § 236.1029; or

(2) Where any train is rerouted onto a track not equipped with a PTC system, the train shall be operated in accordance with the operating rules applicable to the line on which the train is rerouted.

(k) *Rerouting cessation.* The applicable Regional Administrator may order a railroad to cease any rerouting provided under paragraph (g) or (h) of this section.

[75 FR 2699, Jan. 15, 2010, as amended at 75 FR 59117, Sept. 27, 2010; 77 FR 28305, May 14, 2012; 79 FR 49716, Aug. 22, 2014; 81 FR 10128, Feb. 29, 2016]

§ 236.1006 Equipping locomotives operating in PTC territory.

(a) *General.* Except as provided in paragraph (b) of this section, each locomotive, locomotive consist, or train on

any track segment equipped with a PTC system shall be controlled by a locomotive equipped with an onboard PTC apparatus that is fully operative and functioning in accordance with the applicable PTCSP approved under this subpart.

(b) *Exceptions.* (1) Each railroad required to install PTC shall include in its PTCIP specific goals for progressive implementation of onboard systems and deployment of PTC-equipped locomotives such that the safety benefits of PTC are achieved through incremental growth in the percentage of controlling locomotives operating on PTC lines that are equipped with operative PTC onboard equipment. The PTCIP shall include a brief but sufficient explanation of how those goals will be achieved, including assignment of responsibilities within the organization. The goals shall be expressed as the percentage of trains operating on PTC-equipped lines that are equipped with operative onboard PTC apparatus responsive to the wayside, expressed as an annualized (calendar year) percentage for the railroad as a whole.

(2) [Reserved]

(3) A train controlled by a locomotive with an onboard PTC apparatus that has failed en route is permitted to operate in accordance with 49 U.S.C. 20157(j) or § 236.1029, as applicable.

(4) A train operated by a Class II or Class III railroad, including a tourist or excursion railroad, and controlled by a locomotive not equipped with an onboard PTC apparatus is permitted to operate on a PTC-operated track segment:

(i) That either:

(A) Has no regularly scheduled intercity or commuter passenger rail traffic; or

(B) Has regularly scheduled intercity or commuter passenger rail traffic and the applicable PTCIP permits the operation of a train operated by a Class II or III railroad and controlled by a locomotive not equipped with an onboard PTC apparatus;

(ii) Where operations are restricted to four or less such unequipped trains per day, whereas a train conducting a ''turn'' operation (e.g., moving to a point of interchange to drop off or pick up cars and returning to the track owned by a Class II or III railroad) is considered two trains for this purpose; and

(iii) Where each movement shall either:

(A) Not exceed 20 miles in length; or

(B) To the extent any movement exceeds 20 miles in length, such movement is not permitted without the controlling locomotive being equipped with an onboard PTC system after December 31, 2023, and each applicable Class II or III railroad shall report to FRA its progress in equipping each necessary locomotive with an onboard PTC apparatus to facilitate continuation of the movement. The progress reports shall be filed not later than December 31, 2020 and, if all necessary locomotives are not yet equipped, on December 31, 2022.

(5) *Freight yard movements.* For the purpose of freight switching service or freight transfer train service, a locomotive, locomotive consist, or train may operate without onboard PTC apparatus installed or operational where an onboard PTC apparatus is otherwise required by this part only if all of the following six requirements and conditions are met:

(i) The locomotive, locomotive consist, or train must be engaged in freight switching service or freight transfer train service, including yard, local, industrial, and hostling service, movements in connection with the assembling or disassembling of trains, and work trains;

(ii) The movement must originate either:

(A) In a yard; or

(B) Within 20 miles of a yard with the yard as the final destination point;

(iii) The locomotive, locomotive consist, or train shall not travel to a point in excess of 20 miles from its point of entry onto the PTC-equipped main line track;

(iv) The speed of the locomotive, locomotive consist, or train shall not exceed restricted speed, except if:

(A) No other locomotive, locomotive consist, or train is operating on any part of the route without an operational onboard PTC apparatus;

(B) No working limits are established under part 214 of this chapter on any part of the route; and

(C) Either an air brake test under part 232 of this chapter is performed, in which case the locomotive, locomotive consist, or train may proceed at a speed not to exceed 30 miles per hour; or an air brake test under part 232 of this chapter is not performed, in which case the locomotive, locomotive consist, or train may proceed at a speed not to exceed 20 miles per hour;

(v) The speed of the locomotive, locomotive consist, or train shall not exceed restricted speed on PTC-equipped track where the route terminates; and

(vi) The route of the locomotive or train is protected against conflicting operations by the PTC system and sufficient operating rules to protect against train-to-train collisions, as specified in the PTCSP.

(vii) FRA may, in its discretion, approve yard movement procedures other than the yard movement procedures in paragraphs (b)(5)(i) through (b)(5)(vi) of this section in a PTCSP or an RFA that provide an equivalent or greater level of safety as the requirements of paragraphs (b)(5)(i) through (b)(5)(vi) of this section, where such procedures are similar to those of paragraphs (b)(5)(i) through (b)(5)(vi) of this section.

(viii) A locomotive, locomotive consist, or train with an operative onboard PTC apparatus may assist a locomotive, locomotive consist, or train operating without an operative onboard PTC apparatus for purposes such as locomotive malfunction, rescue of locomotive or cars, or to add or remove power, provided that such a movement is made at restricted speed.

(c) When a train movement is conducted under the exceptions described in paragraph (b)(4) of this section, that movement shall be made in accordance with §236.1029.

(d) *Onboard PTC apparatus.* (1) The onboard PTC apparatus shall be so arranged that each member of the crew assigned to perform duties in the locomotive can receive the same PTC information displayed in the same manner and execute any functions necessary to that crew member's duties. The locomotive engineer shall not be required to perform functions related to the PTC system while the train is moving that have the potential to distract the locomotive engineer from performance of other safety-critical duties.

(2) The onboard PTC apparatus may be distributed among multiple locomotives if such functionality is included with the applicable PTCSP approved under this subpart. The controlling locomotive shall be equipped with a fully operative interface that complies with paragraph (d)(1) of this section and is consistent with appendix E of this part.

[75 FR 2699, Jan. 15, 2010, as amended at 79 FR 49716, Aug. 22, 2014; 81 FR 10129, Feb. 29, 2016]

§236.1007 Additional requirements for high-speed service.

(a) A PTC railroad that conducts a passenger operation at or greater than 60 miles per hour or a freight operation at or greater than 50 miles per hour shall have installed a PTC system including or working in concert with technology that includes all of the safety-critical functional attributes of a block signal system meeting the requirements of this part, including appropriate fouling circuits and broken rail detection (or equivalent safeguards).

(b) In addition to the requirements of paragraph (a) of this section, a host railroad that conducts a freight or passenger operation at more than 90 miles per hour shall:

(1) Have an approved PTCSP establishing that the system was designed and will be operated to meet the fail-safe operation criteria described in Appendix C to this part; and

(2) Prevent unauthorized or unintended entry onto the main line from any track not equipped with a PTC system compliant with this subpart by placement of split-point derails or equivalent means integrated into the PTC system; and

(3) Comply with §236.1029(c).

(c) In addition to the requirements of paragraphs (a) and (b) of this section, a host railroad that conducts a freight or passenger operation at more than 125 miles per hour shall have an approved PTCSP accompanied by a document (''HSR–125'') establishing that the system:

(1) Will be operated at a level of safety comparable to that achieved over

the 5 year period prior to the submission of the PTCSP by other train control systems that perform PTC functions required by this subpart, and which have been utilized on high-speed rail systems with similar technical and operational characteristics in the United States or in foreign service, provided that the use of foreign service data must be approved by the Associate Administrator before submittal of the PTCSP; and

(2) Has been designed to detect incursions into the right-of-way, including incidents involving motor vehicles diverting from adjacent roads and bridges, where conditions warrant.

(d) In addition to the requirements of paragraphs (a) through (c) of this section, a host railroad that conducts a freight or passenger operation at more than 150 miles per hour, which is governed by a Rule of Particular Applicability, shall have an approved PTCSP accompanied by a HSR–125 developed as part of an overall system safety plan approved by the Associate Administrator.

(e) A railroad providing existing high-speed passenger service may request in its PTCSP that the Associate Administrator excuse compliance with one or more requirements of this section upon a showing that the subject service has been conducted with a high level of safety.

§ 236.1009 Procedural requirements.

(a) *PTC Implementation Plan (PTCIP).* (1) By April 16, 2010, each host railroad that is required to implement and operate a PTC system in accordance with § 236.1005(b) shall develop and submit in accordance with § 236.1011(a) a PTCIP for implementing a PTC system required under § 236.1005. Filing of the PTCIP shall not exempt the required filings of an NPI, PTCSP, PTCDP, or Type Approval.

(2) After April 16, 2010, a host railroad shall file:

(i) A PTCIP if it becomes a host railroad of a main line track segment for which it is required to implement and operate a PTC system in accordance with § 236.1005(b); or

(ii) A request for amendment (''RFA'') of its current and approved PTCIP in accordance with § 236.1021 if it intends to:

(A) Initiate a new category of service (i.e., passenger or freight); or

(B) Add, subtract, or otherwise materially modify one or more lines of railroad for which installation of a PTC system is required.

(3) The host and tenant railroad(s) shall jointly file a PTCIP that addresses shared track:

(i) If the host railroad is required to install and operate a PTC system on a segment of its track; and

(ii) If the tenant railroad that shares the same track segment would have been required to install a PTC system if the host railroad had not otherwise been required to do so.

(4) If railroads required to file a joint PTCIP are unable to jointly file a PTCIP in accordance with paragraphs (a)(1) and (a)(3) of this section, then each railroad shall:

(i) Separately file a PTCIP in accordance with paragraph (a)(1);

(ii) Notify the Associate Administrator that the subject railroads were unable to agree on a PTCIP to be jointly filed;

(iii) Provide the Associate Administrator with a comprehensive list of all issues not in agreement between the railroads that would prevent the subject railroads from jointly filing the PTCIP; and

(iv) Confer with the Associate Administrator to develop and submit a PTCIP mutually acceptable to all subject railroads.

(5) Each railroad filing a PTCIP shall report annually, by March 31 of each year, and until its PTC system implementation is complete, its progress towards fulfilling the goals outlined in its PTCIP under this part, including progress towards PTC system installation pursuant to § 236.1005 and onboard PTC apparatus installation and use in PTC-equipped track segments pursuant to § 236.1006, as well as impediments to completion of each of the goals.

(b) *Type Approval.* Each host railroad, individually or jointly with others such as a tenant railroad or system supplier, shall file prior to or simultaneously with the filing made in accordance with paragraph (a) of this section:

(1) An unmodified Type Approval previously issued by the Associate Administrator in accordance with § 236.1013 or § 236.1031(b) with its associated docket number;

(2) A PTCDP requesting a Type Approval for:

(i) A PTC system that does not have a Type Approval; or

(ii) A PTC system with a previously issued Type Approval that requires one or more variances;

(3) A PTCSP subject to the conditions set forth in paragraph (c) of this section, with or without a Type Approval; or

(4) A document attesting that a Type Approval is not necessary since the host railroad has no territory for which a PTC system is required under this subpart.

(c) *Notice of Product Intent (NPI).* A railroad may, in lieu of submitting a PTCDP, or referencing an already issued Type Approval, submit an NPI describing the functions of the proposed PTC system. If a railroad elects to file an NPI in lieu of a PTCDP or referencing an existing Type Approval with the PTCIP, and the PTCIP is otherwise acceptable to the Associate Administrator, the Associate Administrator may grant provisional approval of the PTCIP.

(1) A provisional approval of a PTCIP, unless otherwise extended by the Associate Administrator, is valid for a period of 270 days from the date of approval by the Associate Administrator.

(2) The railroad must submit an updated PTCIP with either a complete PTCDP as defined in § 236.1013(a), an updated PTCIP referencing an already approved Type Approval, or a full PTCSP within 270 days after the ''Provisional Approval.''

(i) Within 90 days of receipt of an updated PTCIP that was submitted with an NPI, the Associate Administrator will approve or disapprove of the updated PTCIP and notify in writing the affected railroad. If the updated PTCIP is not approved, the notification will include the plan's deficiencies. Within 30 days of receipt of that notification, the railroad or other entity that submitted the plan shall correct all deficiencies and resubmit the plan in accordance with this section and § 236.1011, as applicable.

(ii) If an update to a ''Provisionally Approved'' PTCIP is not received by the Associate Administrator by the end of the period indicated in this paragraph, the ''Provisional Approval'' given to the PTCIP is automatically revoked. The revocation is retroactive to the date the original PTCIP and NPI were first submitted to the Associate Administrator.

(d) *PTCSP and PTC System Certification.* The following apply to each PTCSP and PTC System Certification.

(1) A PTC System Certification for a PTC system may be obtained by submitting an acceptable PTCSP. If the PTC system is the subject of a Type Approval, the safety case elements contained in the PTCDP may be incorporated by reference into the PTCSP, subject to finalization of the human factors analysis contained in the PTCDP.

(2) Each PTCSP requirement under § 236.1015 shall be supported by information and analysis sufficient to establish that the requirements of this subpart have been satisfied.

(3) If the Associate Administrator finds that the PTCSP and supporting documentation support a finding that the system complies with this part, the Associate Administrator may approve the PTCSP. If the Associate Administrator approves the PTCSP, the railroad shall receive PTC System Certification for the subject PTC system and shall implement the PTC system according to the PTCSP.

(4) A required PTC system shall not:

(i) Be used in service until it receives from FRA a PTC System Certification; and

(ii) Receive a PTC System Certification unless FRA receives and approves an applicable:

(A) PTCSP; or

(B) Request for Expedited Certification (REC) as defined by § 236.1031(a).

(e) *Plan contents.* (1) No PTCIP shall receive approval unless it complies with § 236.1011. No railroad shall receive a Type Approval or PTC System Certification unless the applicable PTCDP or PTCSP, respectively, comply with §§ 236.1013 and 236.1015, respectively.

(2) All materials filed in accordance with this subpart must be in the English language, or have been translated into English and attested as true and correct.

(3) Each filing referenced in this section may include a request for full or partial confidentiality in accordance with § 209.11 of this chapter. If confidentiality is requested as to a portion of any applicable document, then in addition to the filing requirements under § 209.11 of this chapter, the person filing the document shall also file a copy of the original unredacted document, marked to indicate which portions are redacted in the document's confidential version without obscuring the original document's contents.

(f) *Supporting documentation and information.* (1) Issuance of a Type Approval or PTC System Certification is contingent upon FRA's confidence in the implementation and operation of the subject PTC system. This confidence may be based on FRA-monitored field testing or an independent assessment performed in accordance with § 236.1035 or § 236.1017, respectively.

(2) Upon request by FRA, the railroad requesting a Type Approval or PTC System Certification must engage in field testing or independent assessment performed in accordance with § 236.1035 or § 236.1017, respectively, to support the assertions made in any of the plans submitted under this subpart. These assertions include any of the plans' content requirements under this subpart.

(g) *FRA conditions, reconsiderations, and modifications.* (1) As necessary to ensure safety, FRA may attach special conditions to approving a PTCIP or issuing a Type Approval or PTC System Certification.

(2) After granting a Type Approval or PTC System Certification, FRA may reconsider the Type Approval or PTC System Certification upon revelation of any of the following factors concerning the contents of the PTCDP or PTCSP:

(i) Potential error or fraud;

(ii) Potentially invalidated assumptions determined as a result of in-service experience or one or more unsafe events calling into question the safety analysis supporting the approval.

(3) During FRA's reconsideration in accordance with this paragraph, the PTC system may remain in use if otherwise consistent with the applicable law and regulations and FRA may impose special conditions for use of the PTC system.

(4) After FRA's reconsideration in accordance with this paragraph, FRA may:

(i) Dismiss its reconsideration and continue to recognize the existing FRA approved Type Approval or PTC System Certification;

(ii) Allow continued operations under such conditions the Associate Administrator deems necessary to ensure safety; or

(iii) Revoke the Type Approval or PTC System Certification and direct the railroad to cease operations where PTC systems are required under this subpart.

(h) *FRA access.* The Associate Administrator, or that person's designated representatives, shall be afforded reasonable access to monitor, test, and inspect processes, procedures, facilities, documents, records, design and testing materials, artifacts, training materials and programs, and any other information used in the design, development, manufacture, test, implementation, and operation of the system, as well as interview any personnel:

(1) Associated with a PTC system for which a Type Approval or PTC System Certification has been requested or provided; or

(2) To determine whether a railroad has been in compliance with this subpart.

(i) *Foreign regulatory entity verification.* Information that has been certified under the auspices of a foreign regulatory entity recognized by the Associate Administrator may, at the Associate Administrator's sole discretion, be accepted as independently Verified and Validated and used to support each railroad's development of the PTCSP.

(j) *Processing times for PTCDP and PTCSP.*

(1) Within 30 days of receipt of a PTCDP or PTCSP, the Associate Administrator will either acknowledge receipt or acknowledge receipt and request more information.

(2) To the extent practicable, considering the scope, complexity, and novelty of the product or change:

(i) FRA will approve, approve with conditions, or deny the PTCDP within 60 days of the date on which the PTCDP was filed;

(ii) FRA will approve, approve with conditions, or deny the PTCSP within 180 days of the date on which the PTCSP was filed;

(iii) If FRA has not approved, approved with conditions, or denied the PTCDP or PTCSP within the 60-day or 180-day window, as applicable, FRA will provide the submitting party with a statement of reasons as to why the submission has not yet been acted upon and a projected deadline by which an approval or denial will be issued and any further consultations or inquiries will be resolved.

[75 FR 2699, Jan. 15, 2010, as amended at 79 FR 49717, Aug. 22, 2014; 81 FR 10129, Feb. 29, 2016]

§236.1011 PTC Implementation Plan content requirements.

(a) *Contents.* A PTCIP filed pursuant to this subpart shall, at a minimum, describe:

(1) The functional requirements that the proposed system must meet;

(2) How the PTC railroad intends to comply with §§236.1009(c) and (d);

(3) How the PTC system will provide for interoperability of the system between the host and all tenant railroads on the track segments required to be equipped with PTC systems under this subpart and:

(i) Include relevant provisions of agreements, executed by all applicable railroads, in place to achieve interoperability;

(ii) List all methods used to obtain interoperability; and

(iii) Identify any railroads with respect to which interoperability agreements have not been achieved as of the time the plan is filed, the practical obstacles that were encountered that prevented resolution, and the further steps planned to overcome those obstacles;

(4) How, to the extent practical, the PTC system will be implemented to address areas of greater risk to the public and railroad employees before areas of lesser risk;

(5) The sequence and schedule in which track segments will be equipped and the basis for those decisions, and shall at a minimum address the following risk factors by track segment:

(i) Segment traffic characteristics such as typical annual passenger and freight train volume and volume of poison- or toxic-by-inhalation (PIH or TIH) shipments (loads, residue);

(ii) Segment operational characteristics such as current method of operation (including presence or absence of a block signal system), number of tracks, and maximum allowable train speeds, including planned modifications; and

(iii) Route attributes bearing on risk, including ruling grades and extreme curvature;

(6) The following information relating to rolling stock:

(i) What rolling stock will be equipped with PTC technology;

(ii) The schedule to equip that rolling stock by the applicable deadline under §236.1005(b)(7);

(iii) All documents and information required by §236.1006; and

(iv) Unless the tenant railroad is filing its own PTCIP, the host railroad's PTCIP shall:

(A) Attest that the host railroad has made a formal written request to each tenant railroad requesting identification of each item of rolling stock to be PTC system equipped and the date each will be equipped; and

(B) Include each tenant railroad's response to the host railroad's written request made in accordance with paragraph (a)(6)(iv)(A) of this section;

(7) The number of wayside devices required for each track segment and the installation schedule to complete wayside equipment installation by the applicable deadline under §236.1005(b)(7);

(8) Identification of each track segment on the railroad as mainline or non-mainline track. If the PTCIP includes an MTEA, as defined by §236.1019, the PTCIP should identify the tracks included in the MTEA as main line track with a reference to the MTEA;

(9) To the extent the railroad determines that risk-based prioritization required by paragraph (a)(4) of this section is not practical, the basis for this determination; and

(10) The dates the associated PTCDP and PTCSP, as applicable, will be submitted to FRA in accordance with § 236.1009.

(b) *Additional Class I railroad PTCIP requirements.* Each Class I railroad shall include:

(1) In its PTCIP a strategy for full deployment of its PTC system, describing the criteria that it will apply in identifying additional rail lines on its own network, and rail lines of entities that it controls or engages in joint operations with, for which full or partial deployment of PTC technologies is appropriate, beyond those required to be equipped under this subpart. Such criteria shall include consideration of the policies established by 49 U.S.C. 20156 (railroad safety risk reduction program), and regulations issued thereunder, as well as non-safety business benefits that may accrue.

(2) In the Technology Implementation Plan of its Risk Reduction Program, when first required to be filed in accordance with 49 U.S.C. 20156 and any regulation promulgated thereunder, a specification of rail lines selected for full or partial deployment of PTC under the criteria identified in its PTCIP.

(3) Nothing in this paragraph shall be construed to create an expectation or requirement that additional rail lines beyond those required to be equipped by this subpart must be equipped or that such lines will be equipped during the period of primary implementation ending on the applicable deadline under § 236.1005(b)(7).

(4) As used in this paragraph, ''partial implementation'' of a PTC system refers to use, pursuant to subpart H of this part, of technology embedded in PTC systems that does not employ all of the functionalities required by this subpart.

(c) *FRA review.* Within 90 days of receipt of a PTCIP, the Associate Administrator will approve or disapprove of the plan and notify in writing the affected railroad or other entity. If the PTCIP is not approved, the notification will include the plan's deficiencies. Within 30 days of receipt of that notification, the railroad or other entity that submitted the plan shall correct all deficiencies and resubmit the plan in accordance with § 236.1009 and paragraph (a) of this section, as applicable.

(d) *Subpart H.* A railroad that elects to install a PTC system when not required to do so may elect to proceed under this subpart or under subpart H of this part.

(e) Upon receipt of a PTCIP, NPI, PTCDP, or PTCSP, FRA posts on its public web site notice of receipt and reference to the public docket in which a copy of the filing has been placed. FRA may consider any public comment on each document to the extent practicable within the time allowed by law and without delaying implementation of PTC systems.

(f) The PTCIP shall be maintained to reflect the railroad's most recent PTC deployment plans until all PTC system deployments required under this subpart are complete.

[75 FR 2699, Jan. 15, 2010, as amended at 75 FR 59117, Sept. 27, 2010; 81 FR 10129, Feb. 29, 2016]

§ 236.1013 PTC Development Plan and Notice of Product Intent content requirements and Type Approval.

(a) For a PTC system to obtain a Type Approval from FRA, the PTCDP shall be filed in accordance with § 236.1009 and shall include:

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

(2) A description of the railroad operation or categories of operations on which the PTC system is designed to be used, including train movement density (passenger, freight), operating speeds (including a thorough explanation of intended compliance with § 236.1007), track characteristics, and railroad operating rules;

(3) An operational concepts document, including a list with complete descriptions of all functions which the PTC system will perform to enhance or preserve safety;

(4) A document describing the manner in which the PTC system architecture satisfies safety requirements;

(5) A preliminary human factors analysis, including a complete description of all human-machine interfaces and the impact of interoperability requirements on the same;

(6) An analysis of the applicability to the PTC system of the requirements of subparts A through G of this part that may no longer apply or are satisfied by the PTC system using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled;

(7) A prioritized service restoration and mitigation plan and a description of the necessary security measures for the system;

(8) A description of target safety levels (e.g., MTTHE for major subsystems as defined in subpart H of this part), including requirements for system availability and a description of all backup methods of operation and any critical assumptions associated with the target levels;

(9) A complete description of how the PTC system will enforce authorities and signal indications;

(10) A description of the deviation which may be proposed under §236.1029(c), if applicable; and

(11) A complete description of how the PTC system will appropriately and timely enforce all integrated hazard detectors in accordance with §236.1005(c)(3), if applicable.

(b) If the Associate Administrator finds that the system described in the PTCDP would satisfy the requirements for PTC systems under this subpart and that the applicant has made a reasonable showing that a system built to the stated requirements would achieve the level of safety mandated for such a system under §236.1015, the Associate Administrator may grant a numbered Type Approval for the system.

(c) Each Type Approval shall be valid for a period of 5 years, subject to automatic and indefinite extension provided that at least one PTC System Certification using the subject PTC system has been issued within that period and not revoked.

(d) The Associate Administrator may prescribe special conditions, amendments, and restrictions to any Type Approval as necessary for safety.

(e) If submitted, an NPI must contain the following information:

(1) A description of the railroad operation or categories of operations on which the proposed PTC system is designed to be used, including train movement density (passenger, freight), operating speeds (including a thorough explanation of intended compliance with §236.1007), track characteristics, and railroad operating rules;

(2) An operational concepts document, including a list with complete descriptions of all functions that the proposed PTC system will perform to enhance or preserve safety;

(3) A description of target safety levels (e.g., MTTHE for major subsystems as defined in subpart H of this part), including requirements for system availability and a description of all backup methods of operation and any critical assumptions associated with the target levels;

(4) A complete description of how the proposed PTC system will enforce authorities and signal indications; and

(5) A complete description of how the proposed PTC system will appropriately and timely enforce all integrated hazard detectors in accordance with §236.1005(c)(3), if applicable.

§236.1015 PTC Safety Plan content requirements and PTC System Certification.

(a) Before placing a PTC system required under this part in service, the host railroad must submit to FRA a PTCSP and receive a PTC System Certification. If the Associate Administrator finds that the PTCSP and supporting documentation support a finding that the system complies with this part, the Associate Administrator approves the PTCSP and issues a PTC System Certification. Receipt of a PTC System Certification affirms that the PTC system has been reviewed and approved by FRA in accordance with, and meets the requirements of, this part.

(b) A PTCSP submitted under this subpart may reference and utilize in accordance with this subpart any Type Approval previously issued by the Associate Administrator to any railroad, provided that the railroad:

(1) Maintains a continually updated PTCPVL pursuant to § 236.1023;

(2) Shows that the supplier from which they are procuring the PTC system has established and can maintain a quality control system for PTC system design and manufacturing acceptable to the Associate Administrator. The quality control system must include the process for the product supplier or vendor to promptly and thoroughly report any safety-relevant failure and previously unidentified hazards to each railroad using the product; and

(3) Provides the applicable licensing information.

(c) A PTCSP submitted in accordance with this subpart shall:

(1) Include the FRA approved PTCDP or, if applicable, the FRA issued Type Approval;

(2)(i) Specifically and rigorously document each variance, including the significance of each variance between the PTC system and its applicable operating conditions as described in the applicable PTCDP from that as described in the PTCSP, and attest that there are no other such variances; or

(ii) Attest that there are no variances between the PTC system and its applicable operating conditions as described in the applicable PTCDP from that as described in the PTCSP; and

(3) Attest that the system was otherwise built in accordance with the applicable PTCDP and PTCSP and achieves the level of safety represented therein.

(d) A PTCSP shall include the same information required for a PTCDP under § 236.1013(a). If a PTCDP has been filed and approved prior to filing of the PTCSP, the PTCSP may incorporate the PTCDP by reference, with the exception that a final human factors analysis shall be provided. The PTCSP shall contain the following additional elements:

(1) A hazard log consisting of a comprehensive description of all safety-relevant hazards not previously addressed by the vendor or supplier to be addressed during the life-cycle of the PTC system, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence);

(2) A description of the safety assurance concepts that are to be used for system development, including an explanation of the design principles and assumptions;

(3) A risk assessment of the as-built PTC system described;

(4) A hazard mitigation analysis, including a complete and comprehensive description of each hazard and the mitigation techniques used;

(5) A complete description of the safety assessment and Verification and Validation processes applied to the PTC system, their results, and whether these processes address the safety principles described in Appendix C to this part directly, using other safety criteria, or not at all;

(6) A complete description of the railroad's training plan for railroad and contractor employees and supervisors necessary to ensure safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the PTC system;

(7) 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 PTC system on the railroad and establish safety-critical hazards are appropriately mitigated. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations;

(8) A complete description of any additional warning to be placed in the Operations and Maintenance Manual in the same manner specified in § 236.919 and all warning labels to be placed on equipment as necessary to ensure safety;

(9) A complete description of the configuration or revision control measures designed to ensure that the railroad or its contractor does not adversely affect the safety-functional requirements and that safety-critical hazard mitigation processes are not compromised as a result of any such change;

(10) 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;

(11) A complete description of all post-implementation testing (validation) and monitoring procedures, including the intervals necessary to establish that safety-functional requirements, safety-critical hazard mitigation processes, and safety-critical tolerances are not compromised over time, through use, or after maintenance (adjustment, repair, or replacement) is performed;

(12) A complete description of each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, adjustments, repairs, or replacements, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards (*see* §236.1037);

(13) A safety analysis to determine whether, when the system is in operation, any risk remains of an unintended incursion into a roadway work zone due to human error. If the analysis reveals any such risk, the PTCDP and PTCSP shall describe how that risk will be mitigated;

(14) A more detailed description of any alternative arrangements as already provided under §236.1005(a)(1)(i).

(15) A complete description of how the PTC system will enforce authorities and signal indications, unless already completely provided for in the PTCDP;

(16) A description of how the PTCSP complies with §236.1019(f), if applicable;

(17) A description of any deviation in operational requirements for en route failures as specified under §236.1029(c), if applicable and unless already completely provided for in the PTCDP;

(18) A complete description of how the PTC system will appropriately and timely enforce all integrated hazard detectors in accordance with §236.1005;

(19) An emergency and planned maintenance temporary rerouting plan indicating how operations on the subject PTC system will take advantage of the benefits provided under §236.1005(g) through (k); and

(20) The documents and information required under §§236.1007 and 236.1033.

(21) A list of each location where a locomotive with a failed onboard PTC apparatus will be regularly be exchanged or repaired pursuant to §236.1029(b)(6) and a list of each movement that could take place pursuant to §236.1029(b)(6) if the movement potentially could exceed 500 miles.

(e) The following additional requirements apply to:

(1) *Non-vital overlay.* A PTC system proposed as an overlay on the existing method of operation and not built in accordance with the safety assurance principles set forth in appendix C of this part must, to the satisfaction of the Associate Administrator, be shown to:

(i) Reliably execute the functions set forth in §236.1005;

(ii) Obtain at least 80 percent reduction of the risk associated with accidents preventable by the functions set forth in §236.1005, when all effects of the change associated with the PTC system are taken into account. The supporting risk assessment shall evaluate all intended changes in railroad operations coincident with the introduction of the new system; and

(iii) Maintain a level of safety for each subsequent system modification that is equal to or greater than the level of safety for the previous PTC systems.

(2) *Vital overlay.* A PTC system proposed on a newly constructed track or as an overlay on the existing method of operation and built in accordance with the safety assurance principles set forth in appendix C of this part must, to the satisfaction of the Associate Administrator, be shown to:

(i) Reliably execute the functions set forth in §236.1005; and

(ii) Have sufficient documentation to demonstrate that the PTC system, as built, fulfills the safety assurance principles set forth in appendix C of this part. The supporting risk assessment may be abbreviated as that term is used in subpart H of this part.

(3) *Stand-alone.* A PTC system proposed on a newly constructed track, an existing track for which no signal system exists, as a replacement for an existing signal or train control system, or otherwise to replace or materially

modify the existing method of operation, shall:

(i) Reliably execute the functions required by §236.1005 and be demonstrated to do so to FRA's satisfaction; and

(ii) Have a PTCSP establishing, with a high degree of confidence, that the system will not introduce new hazards that have not been mitigated. The supporting risk assessment shall evaluate all intended changes in railroad operations in relation to the introduction of the new system and shall examine in detail the direct and indirect effects of all changes in the method of operations.

(4) *Mixed systems.* If a PTC system combining overlay, stand-alone, vital, or non-vital characteristics is proposed, the railroad shall confer with the Associate Administrator regarding appropriate structuring of the safety case and analysis.

(f) When determining whether the PTCSP fulfills the requirements under paragraph (d) of this section, the Associate Administrator may consider all available evidence concerning the reliability and availability of the proposed system and any and all safety consequences of the proposed changes. In any case where the PTCSP lacks adequate data regarding safety impacts of the proposed changes, the Associate Administrator may request the necessary data from the applicant. If the requested data is not provided, the Associate Administrator may find that potential hazards could or will arise.

(g) If a PTCSP applies to a system designed to replace an existing certified PTC system, the PTCSP will be approved provided that the PTCSP establishes with a high degree of confidence that the new system will provide a level of safety not less than the level of safety provided by the system to be replaced.

(h) When reviewing the issue of the potential data errors (for example, errors arising from data supplied from other business systems needed to execute the braking algorithm, survey data needed for location determination, or mandatory directives issued through the computer-aided dispatching system), the PTCSP must include a careful identification of each of the risks and a discussion of each applicable mitigation. In an appropriate case, such as a case in which the residual risk after mitigation is substantial or the underlying method of operation will be significantly altered, the Associate Administrator may require submission of a quantitative risk assessment addressing these potential errors.

[75 FR 2699, Jan. 15, 2010, as amended at 79 FR 49717, Aug. 22, 2014]

§236.1017 Independent third party Verification and Validation.

(a) The PTCSP must be supported by an independent third-party assessment when the Associate Administrator concludes that it is necessary based upon the criteria set forth in §236.913, with the exception that consideration of the methodology used in the risk assessment (§236.913(g)(2)(vii)) shall apply only to the extent that a comparative risk assessment was required. To the extent practicable, FRA makes this determination not later than review of the PTCIP and the accompanying PTCDP or PTCSP. If an independent assessment is required, the assessment may apply to the entire system or a designated portion of the system.

(b) If a PTC system is to undergo an independent assessment in accordance with this section, the host railroad may submit to the Associate Administrator a written request that FRA confirm whether a particular entity would be considered an independent third party pursuant to this section. The request should include supporting information identified in paragraph (c) of this section. FRA may request further information to make a determination or provide its determination in writing.

(c) 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 PTC system supplier and vendor. An entity that is owned or controlled by the supplier or vendor, that is under common ownership or control with the supplier or vendor, or that is otherwise involved in the development of the PTC system is not considered ''independent'' within the meaning of this section.

(d) The independent third-party assessment shall, at a minimum, consist of the activities and result in the production of documentation meeting the requirements of Appendix F to this part, unless excepted by this part or by FRA order or waiver.

(e) Information provided that has been certified under the auspices of a foreign railroad regulatory entity recognized by the Associate Administrator may, at the Associate Administrator's discretion, be accepted as having been independently verified.

§236.1019 Main line track exceptions.

(a) *Scope and procedure.* This section pertains exclusively to exceptions from the rule that trackage over which scheduled intercity and commuter passenger service is provided is considered main line track requiring installation of a PTC system. One or more intercity or commuter passenger railroads, or freight railroads conducting joint passenger and freight operation over the same segment of track may file a main line track exclusion addendum (''MTEA'') to its PTCIP requesting to designate track as not main line subject to the conditions set forth in paragraphs (b) or (c) of this section. No track shall be designated as yard or terminal unless it is identified in an MTEA that is part of an FRA approved PTCIP.

(b) *Passenger terminal exception.* FRA will consider an exception in the case of trackage used exclusively as yard or terminal tracks by or in support of regularly scheduled intercity or commuter passenger service where the MTEA describes in detail the physical boundaries of the trackage in question, its use and characteristics (including track and signal charts) and all of the following apply:

(1) The maximum authorized speed for all movements is not greater than 20 miles per hour, and that maximum is enforced by any available onboard PTC equipment within the confines of the yard or terminal;

(2) Interlocking rules are in effect prohibiting reverse movements other than on signal indications without dispatcher permission; and

(3) Either of the following conditions exists:

(i) No freight operations are permitted; or

(ii) Freight operations are permitted but no passengers will be aboard passenger trains within the defined limits.

(c) *Limited operations exception.* FRA will consider an exception in the case of a track segment used for limited operations (operating in accordance with §236.0 of this part) under one of the following sets of conditions:

(1) The trackage is used for limited operations by at least one passenger railroad subject to at least one of the following conditions:

(i) All trains are limited to restricted speed;

(ii) Temporal separation of passenger and other trains is maintained as provided in paragraph (e) of this section; or

(iii) Passenger service is operated under a risk mitigation plan submitted by all railroads involved in the joint operation and approved by FRA. The risk mitigation plan must be supported by a risk assessment establishing that the proposed mitigations will achieve a level of safety not less than the level of safety that would obtain if the operations were conducted under paragraph (c)(1) or (c)(2) of this section.

(2) Passenger service is operated on a segment of track of a freight railroad that is not a Class I railroad on which less than 15 million gross tons of freight traffic is transported annually and on which one of the following conditions applies:

(i) If the segment is unsignaled and no more than four regularly scheduled passenger trains are operated during a calendar day, or

(ii) If the segment is signaled (e.g., equipped with a traffic control system, automatic block signal system, or cab signal system) and no more than 12 regularly scheduled passenger trains are operated during a calendar day.

(3) Not more than four passenger trains per day are operated on a segment of track of a Class I freight railroad on which less than 15 million gross tons of freight traffic is transported annually.

(d) A limited operations exception under paragraph (c) is subject to FRA review and approval. FRA may require a collision hazard analysis to identify

hazards and may require that specific mitigations be undertaken. Operations under any such exception shall be conducted subject to the terms and conditions of the approval. Any main line track exclusion is subject to periodic review.

(e) *Temporal separation.* As used in this section, temporal separation means that limited passenger and freight operations do not operate on any segment of shared track during the same period and also refers to the processes or physical arrangements, or both, in place to ensure that temporal separation is established and maintained at all times. The use of exclusive authorities under mandatory directives is not, by itself, sufficient to establish that temporal separation is achieved. Procedures to ensure temporal separation shall include verification checks between passenger and freight operations and effective physical means to positively ensure segregation of passenger and freight operations in accordance with this paragraph.

(f) *PTCSP requirement.* No PTCSP—filed after the approval of a PTCIP with an MTEA—shall be approved by FRA unless it attests that no changes, except for those included in an FRA approved RFA, have been made to the information in the PTCIP and MTEA required by paragraph (b) or (c) of this section.

(g) *Designation modifications.* If subsequent to approval of its PTCIP or PTCSP the railroad seeks to modify which track or tracks should be designated as main line or not main line, it shall request modification of its PTCIP or PTCSP, as applicable, in accordance with §236.1021.

[75 FR 2699, Jan. 15, 2010, as amended at 75 FR 59117, Sept. 27, 2010]

§236.1020 [Reserved]

§236.1021 Discontinuances, material modifications, and amendments.

(a) No changes, as defined by this section, to a PTC system, PTCIP, PTCDP, or PTCSP, shall be made unless:

(1) The railroad files a request for amendment (''RFA'') to the applicable PTCIP, PTCDP, or PTCSP with the Associate Administrator; and

(2) The Associate Administrator approves the RFA.

(b) After approval of an RFA in accordance with paragraph (a) of this section, the railroad shall immediately adopt and comply with the amendment.

(c) In lieu of a separate filing under part 235 of this chapter, a railroad may request approval of a discontinuance or material modification of a signal or train control system by filing an RFA to its PTCIP, PTCDP, or PTCSP with the Associate Administrator.

(d) An RFA made in accordance with this section will not be approved by FRA unless the request includes:

(1) The information listed in §235.10 of this chapter and the railroad provides FRA upon request any additional information necessary to evaluate the RFA (see §235.12), including:

(2) The proposed modifications;

(3) The reasons for each modification;

(4) The changes to the PTCIP, PTCDP, or PTCSP, as applicable;

(5) Each modification's effect on PTC system safety;

(6) An approximate timetable for filing of the PTCDP, PTCSP, or both, if the amendment pertains to a PTCIP; and

(7) An explanation of whether each change to the PTCSP is planned or unplanned.

(i) Unplanned changes that affect the Type Approval's PTCDP require submission and approval in accordance with §236.1013 of a new PTCDP, followed by submission and approval in accordance with §236.1015 of a new PTCSP for the PTC system.

(ii) Unplanned changes that do not affect the Type Approval's PTCDP require submission and approval of a new PTCSP.

(iii) Unplanned changes are changes affecting system safety that have not been documented in the PTCSP. The impact of unplanned changes on PTC system safety has not yet been determined.

(iv) Planned changes may be implemented after they have undergone suitable regression testing to demonstrate, to the satisfaction of the Associate Administrator, they have been correctly implemented and their implementation does not degrade safety.

(v) Planned changes are changes affecting system safety in the PTCSP and have been included in all required analysis under §236.1015. The impact of these changes on the PTC system's safety has been incorporated as an integral part of the approved PTCSP safety analysis.

(e) If the RFA includes a request for approval of a discontinuance or material modification of a signal or train control system, FRA will publish a notice in the FEDERAL REGISTER of the application and will invite public comment in accordance with part 211 of this chapter.

(f) When considering the RFA, FRA will review the issue of the discontinuance or material modification and determine whether granting the request is in the public interest and consistent with railroad safety, taking into consideration all changes in the method of operation and system functionalities, both within normal PTC system availability and in the case of a system failed state (unavailable), contemplated in conjunction with installation of the PTC system. The railroad submitting the RFA must, at FRA's request, perform field testing in accordance with §236.1035 or engage in Verification and Validation in accordance with §236.1017.

(g) FRA may issue at its discretion a new Type Approval number for a PTC system modified under this section.

(h) *Changes requiring filing of an RFA.* Except as provided by paragraph (i), an RFA shall be filed to request the following:

(1) Discontinuance of a PTC system, or other similar appliance or device;

(2) Decrease of the PTC system's limits (e.g., exclusion or removal of a PTC system on a track segment);

(3) Modification of a safety critical element of a PTC system; or

(4) Modification of a PTC system that affects the safety critical functionality of any other PTC system with which it interoperates.

(i) *Discontinuances not requiring the filing of an RFA.* It is not necessary to file an RFA for the following discontinuances:

(1) Removal of a PTC system from track approved for abandonment by formal proceeding;

(2) Removal of PTC devices used to provide protection against unusual contingencies such as landslide, burned bridge, high water, high and wide load, or tunnel protection when the unusual contingency no longer exists;

(3) Removal of the PTC devices that are used on a movable bridge that has been permanently closed by the formal approval of another government agency and is mechanically secured in the closed position for rail traffic; or

(4) Removal of the PTC system from service for a period not to exceed 6 months that is necessitated by catastrophic occurrence such as derailment, flood, fire, or hurricane, or earthquake.

(j) *Changes not requiring the filing of an RFA.* When the resultant change to the PTC system will comply with an approved PTCSP of this part, it is not necessary to file for approval to decrease the limits of a system when it involves the:

(1) Decrease of the limits of a PTC system when interlocked switches, derails, or movable-point frogs are not involved;

(2) Removal of an electric or mechanical lock, or signal used in lieu thereof, from hand-operated switch in a PTC system where train speed over such switch does not exceed 20 miles per hour, and use of those devices has not been part of the considerations for approval of a PTCSP; or

(3) Removal of an electric or mechanical lock, or signal used in lieu thereof, from a hand-operated switch in a PTC system where trains are not permitted to clear the main track at such switch and use of those devices has not been a part of the considerations for approval of a PTCSP.

(k) *Modifications not requiring the filing of an RFA.* When the resultant arrangement will comply with an approved PTCSP of this part, it is not necessary to file an application for approval of the following modifications:

(1) A modification that is required to comply with an order of the Federal Railroad Administration or any section of part 236 of this title;

(2) Installation of devices used to provide protection against unusual contingencies such as landslide, burned

bridges, high water, high and wide loads, or dragging equipment;

(3) Elimination of existing track other than a second main track;

(4) Extension or shortening of a passing siding; or

(5) The temporary or permanent arrangement of existing systems necessitated by highway-rail grade separation construction. Temporary arrangements shall be removed within six months following completion of construction.

§ 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 PTCSP 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.

(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 PTCSP 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 PTCSP 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 PTCSP and those that had not previously been identified in the PTCSP. If the frequency of the safety-relevant hazard exceeds the thresholds set forth in the PTCSP, 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 PTCSP.

(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 expeditious 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;

(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.

§ 236.1029 PTC system use and failures.

(a) When any safety-critical PTC system 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 is completed, a railroad shall take appropriate action as specified in its PTCSP.

(b) *En route failures.* Except as provided in paragraphs (c) and (g) of this section, where a controlling locomotive that is operating in, or is to be operated within, a PTC-equipped track segment experiences PTC system failure or the PTC system is otherwise cut out while en route (i.e., after the train has departed its initial terminal), the train may only continue in accordance with all of the following:

(1) Except as provided in paragraph (b)(5) of this section, where no block signal system is in use, the train may proceed at a speed not to exceed 40 miles per hour; however, if the involved train is transporting one or more cars containing PIH materials, excluding those cars containing only a residue of PIH materials, the train may only proceed at a speed not to exceed 30 miles per hour.

(2) Where a block signal system is in place:

(i) A passenger train may proceed at a speed not to exceed 59 miles per hour;

(ii) A freight train transporting one or more cars containing PIH materials, excluding those cars containing only a residue of PIH materials, may proceed at a speed not to exceed 40 miles per hour; and

(iii) Any other freight train may proceed at a speed not to exceed 49 miles per hour.

(3) Where a cab signal system with an automatic train control system is in use, the train may proceed at a speed not to exceed 79 miles per hour.

(4) A report of the failure or cut-out must be made to a designated railroad officer of the host railroad as soon as safe and practicable.

(5) Where the PTC system is the exclusive method of delivering mandatory directives, an absolute block must be established in advance of the train as soon as safe and practicable, and the train shall not exceed restricted speed until the absolute block in advance of the train is established.

(6) Where the failure or cut-out is a result of a defective onboard PTC apparatus, the train may continue no farther than the next forward designated location for the repair or exchange of onboard PTC apparatuses.

(c) *Exception for alternative system failure procedure.* A railroad may submit for approval a PTCSP, an RFA, or an Order of Particular Applicability with an alternative system failure procedure other than that required by paragraph (b) of this section. FRA may, in its discretion, approve such an alternative system failure procedure if it provides similar requirements of, and an equivalent or greater level of safety as, the requirements of paragraph (b) of this section.

(d) Each railroad shall comply with all provisions in the applicable PTCDP and PTCSP for each PTC system it uses and shall operate within the scope of initial operational assumptions and predefined changes identified.

(e) The normal functioning of any safety-critical PTC system must not be interfered with in testing or otherwise without first taking measures to provide for the safe movement of trains, locomotives, roadway workers, and on-track equipment that depend on the normal functioning of the system.

(f) [Reserved]

(g) *Temporary exceptions.* From October 21, 2014 through the 24 months following the date of required PTC system implementation established by section 20157 of title 49 of the United States Code—

(1) A railroad's PTCSP or Order of Particular Applicability may provide for compliance with the en route failure requirements of § 236.567 instead of paragraph (b) of this section where a controlling locomotive that is operating in, or is to be operated within, a PTC-equipped track segment experiences PTC system failure or the PTC system is otherwise cut out while en route;

(2) A train may proceed as prescribed under either paragraph (b) of this section or §236.567 where the PTC system fails to initialize for any reason prior to the train's departure from its initial terminal; and

(3) A railroad's PTCSP may provide for the temporary disabling of PTC system service where necessary to perform PTC system repair or maintenance. In this paragraph (g)(3), ''PTC system service'' does not refer to the failure of the onboard PTC apparatus for a single locomotive, locomotive consist, or train.

(i) The PTCSP shall specify appropriate operating rules to apply when the PTC system is temporarily disabled in accordance with this paragraph (g)(3).

(ii) The railroad shall make reasonable efforts to schedule the temporary disabling of PTC system service for times posing the least risk to railroad safety.

(iii) The railroad shall provide notice to the FRA regional office having jurisdiction over that territory at least 7 days in advance of planned temporary disabling of PTC system service and contemporaneous notice for unplanned temporary disabling of PTC system service.

(iv) The PTC system that is temporarily disabled in accordance with this paragraph (g)(3) shall be placed back into service without undue delay.

(h) *Annual report of system failures.* Annually, by April 16 of each year following the date of required PTC system implementation established by section 20157 of title 49 of the United States Code, each railroad shall provide FRA with a report of the number of PTC failures that occurred during the previous calendar year. The report shall identify failures by category, including but not limited to locomotive, wayside, communications, and back office system failures.

[75 FR 2699, Jan. 15, 2010, as amended at 79 FR 49717, Aug. 22, 2014]

§236.1031 Previously approved PTC systems.

(a) Any PTC system fully implemented and operational prior to March 16, 2010, may receive PTC System Certification if the applicable PTC railroad, or one or more system suppliers and one or more PTC railroads, submits a Request for Expedited Certification (REC) letter to the Associate Administrator. The REC letter must do one of the following:

(1) Reference a product safety plan (PSP) approved by FRA under subpart H of this part and include a document fulfilling the requirements under §§236.1011 and 236.1013 not already included in the PSP;

(2) Attest that the PTC system has been approved by FRA and in operation for at least 5 years and has already received an assessment of Verification and Validation from an independent third party under part 236 or a waiver supporting such operation; or

(3) Attest that the PTC system is recognized under an Order issued prior to March 16, 2010.

(b) If an REC letter conforms to paragraph (a)(1) of this section, the Associate Administrator, at his or her sole discretion, may also issue a new Type Approval for the PTC system.

(c) In order to receive a Type Approval or PTC System Certification under paragraph (a) or (b) of this section, the PTC system must be shown to reliably execute the functionalities required by §§236.1005 and 236.1007 and otherwise conform to this subpart.

(d) Previous approval or recognition of a train control system, together with an established service history, may, at the request of the PTC railroad, and consistent with available safety data, be credited toward satisfaction of the safety case requirements set forth in this part for the PTCSP with respect to all functionalities and implementations contemplated by the approval or recognition.

(e) To the extent that the PTC system proposed for implementation under this subpart is different in significant detail from the system previously approved or recognized, the changes shall be fully analyzed in the PTCDP or PTCSP as would be the case absent prior approval or recognition.

(f) As used in this section—

(1) *Approved* refers to approval of a Product Safety Plan under subpart H of this part.

(2) *Recognized* refers to official action permitting a system to be implemented

for control of train operations under an FRA order or waiver, after review of safety case documentation for the implementation.

(g) Upon receipt of an REC, FRA will consider all safety case information to the extent feasible and appropriate, given the specific facts before the agency. Nothing in this section limits reuse of any applicable safety case information by a party other than the party receiving:

(1) A prior approval or recognition referred to in this section; or

(2) A Type Approval or PTC System Certification under this subpart.

§ 236.1033 Communications and security requirements.

(a) All wireless communications between the office, wayside, and onboard components in a PTC system shall provide cryptographic message integrity and authentication.

(b) Cryptographic keys required under paragraph (a) of this section shall:

(1) Use an algorithm approved by the National Institute of Standards (NIST) or a similarly recognized and FRA approved standards body;

(2) Be distributed using manual or automated methods, or a combination of both; and

(3) Be revoked:

(i) If compromised by unauthorized disclosure of the cleartext key; or

(ii) When the key algorithm reaches its lifespan as defined by the standards body responsible for approval of the algorithm.

(c) The cleartext form of the cryptographic keys shall be protected from unauthorized disclosure, modification, or substitution, except during key entry when the cleartext keys and key components may be temporarily displayed to allow visual verification. When encrypted keys or key components are entered, the cryptographically protected cleartext key or key components shall not be displayed.

(d) Access to cleartext keys shall be protected by a tamper resistant mechanism.

(e) Each railroad electing to also provide cryptographic message confidentiality shall:

(1) Comply with the same requirements for message integrity and authentication under this section; and

(2) Only use keys meeting or exceeding the security strength required to protect the data as defined in the railroad's PTCSP and required under § 236.1013(a)(7).

(f) Each railroad, or its vendor or supplier, shall have a prioritized service restoration and mitigation plan for scheduled and unscheduled interruptions of service. This plan shall be included in the PTCDP or PTCSP as required by §§ 236.1013 or 236.1015, as applicable, and made available to FRA upon request, without undue delay, for restoration of communication services that support PTC system services.

(g) Each railroad may elect to impose more restrictive requirements than those in this section, consistent with interoperability requirements specified in the PTCSP for the system.

§ 236.1035 Field testing requirements.

(a) Before any field testing of an uncertified PTC system, or a product of an uncertified PTC system, or any regression testing of a certified PTC system is conducted on the general rail system, the railroad requesting the testing must provide:

(1) A complete description of the PTC system;

(2) An operational concepts document;

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

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

(5) The date the proposed testing shall begin;

(6) The test locations; and

(7) The effect on the current method of operation the PTC system will or may have under test.

(b) FRA may impose additional testing conditions that it believes may be necessary for the safety of train operations.

(c) Relief from regulations other than from subparts A through G of this part that the railroad believes are necessary

to support the field testing, must be requested in accordance with part 211 of this title.

§236.1037 Records retention.

(a) Each railroad with a PTC system required to be installed under this subpart shall maintain at a designated office on the railroad:

(1) A current copy of each FRA approved Type Approval, if any, PTCDP, and PTCSP that it holds;

(2) Adequate documentation to demonstrate that the PTCSP and PTCDP meet the safety requirements of this subpart, including the risk assessment;

(3) An Operations and Maintenance Manual, pursuant to §236.1039; and

(4) Training and testing records pursuant to §236.1043(b).

(b) Results of inspections and tests specified in the PTCSP and PTCDP must be recorded pursuant to §236.110.

(c) Each contractor providing services relating to the testing, maintenance, or operation of a PTC system required to be installed under this subpart shall maintain at a designated office training records required under §236.1039(b).

(d) After the PTC system is placed in service, the railroad shall maintain a database of all safety-relevant hazards as set forth in the PTCSP and PTCDP and those that had not been previously identified in either document. If the frequency of the safety-relevant hazards exceeds the threshold set forth in either of these documents, 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, 1200 New Jersey Ave, SE, 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 each safety-relevant hazard to below the threshold set forth in the PTCSP and PTCDP; and

(3) Provide a final report when the inconsistency is resolved 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 PTCSP and PTCDP.

§236.1039 Operations and Maintenance Manual.

(a) The railroad shall catalog and maintain all documents as specified in the PTCDP and PTCSP for the installation, maintenance, repair, modification, inspection, and testing of the PTC system 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 PTC systems must be adequate in detail and must be made available for inspection by FRA and FRA-certified state inspectors where such PTC systems 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 PTCDP and PTCSP.

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

(e) Each railroad shall designate in its Operations and Maintenance Manual an appropriate railroad officer responsible for issues relating to scheduled interruptions of service contemplated by §236.1029.

§236.1041 Training and qualification program, general.

(a) *Training program for PTC personnel.* Employers shall establish and implement training and qualification programs for PTC systems subject to this subpart. These programs must meet the minimum requirements set forth in the PTCDP and PTCSP in §§236.1039 through 236.1045, 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 PTC systems, 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) *Competencies.* 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 operation and maintenance of the PTC system.

§ 236.1043 Task analysis and basic requirements.

(a) *Training structure and delivery.* As part of the program required by § 236.1041, 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 PTC systems. 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 and evaluation 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 § 236.1041(a) to successfully complete a training curriculum and pass an examination that covers the PTC system 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 and evaluation at intervals specified in the PTCDP and PTCSP 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 § 236.1041(a)(1) verifying the adequacy of the training material and its validity with respect to current railroads PTC systems and operations.

(b) *Training records.* 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

§ 236.1045 Training specific to office control personnel.

(a) Any person responsible for issuing or communicating mandatory directives in territory where PTC systems are or will be in use shall be trained in the following areas, as applicable:

(1) 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;

(2) 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

(3) 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.

(b) [Reserved]

§236.1047 Training specific to locomotive engineers and other operating personnel.

(a) *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 shall be defined in the PTCDP as well as the PTCSP. The following elements shall 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 and testing (part 217) 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) *Locomotive engineer training.* Training required under this subpart for a locomotive engineer, together with required records, shall be integrated into the program of training required by part 240 of this chapter.

(c) *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 PTCDP and PTCSP shall identify all safety hazards to be mitigated by the locomotive engineer.

(2) The PTCDP and PTCSP shall 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 §236.1043(a)(2), develop failure scenarios which incorporate the safety hazards identified in the PTCDP and PTCSP including the return of train operations to a fully manual mode;

(ii) Provide training, consistent with §236.1047(a), for safe train operations under all failure scenarios and identified safety hazards that affect train operations;

(iii) Provide training, consistent with §236.1047(a), for safe train operations under manual control; and

(iv) Consistent with §236.1047(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 FRA. The PTCDP and PTCSP shall designate the appropriate frequency when manual operation, starting, and stopping must be conducted, and the appropriate frequency of simulated manual operation.

(d) *Conductor training.* Training required under this subpart for a conductor, together with required records, shall be integrated into the program of training required under this chapter.

§ 236.1049 Training specific to roadway workers.

(a) *Roadway worker training.* Training required under this subpart for a roadway worker shall 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 § 236.1043. This training shall provide instruction for roadway workers who provide protection for themselves or roadway work groups.

(b) *Training subject areas.* (1) Instruction for roadway workers shall 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 all roadway workers working in territories where PTC is required under this subpart shall 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 A TO PART 236—CIVIL PENALTIES [1, 2]

Section	Violation	Willful violation
Subpart A—Rules and Instructions—All Systems		
General:		
236.0 Applicability, minimum requirements	$2,500	$5,000
236.1 Plans, where kept	1,000	2,000
236.2 Grounds	1,000	2,000
236.3 Locking of signal apparatus housings:		
(a) Power interlocking machine cabinet not secured against unauthorized entry	2,500	5,000
(b) other violations	1,000	2,000
236.4 Interference with normal functioning of device	5,000	7,500
236.5 Design of control circuits on closed circuit principle	1,000	2,000
236.6 Hand-operated switch equipped with switch circuit controller	1,000	2,000
236.7 Circuit controller operated by switch-and-lock movement	1,000	2,000
236.8 Operating characteristics of electro-magnetic, electronic, or electrical apparatus	1,000	2,000
236.9 Selection of circuits through indicating or annunciating instruments	1,000	2,000
236.10 Electric locks, force drop type; where required	1,000	2,000
236.11 Adjustment, repair, or replacement of component	2,500	5,000
236.12 Spring switch signal protection; where required	1,000	2,000
236.13 Spring switch; selection of signal control circuits through circuit controller	1,000	2,000
236.14 Spring switch signal protection; requirements	1,000	2,000
236.15 Timetable instructions	1,000	2,000
236.16 Electric lock, main track releasing circuit:.		
(a) Electric lock releasing circuit on main track extends into fouling circuit where turnout not equipped with derail at clearance point either pipe-connected to switch or independently locked, electrically	2,500	5,000
(b) other violations	1,000	2,000
236.17 Pipe for operating connections, requirements	1,000	2,000
236.18 Software management control plan:.		
Failure to develop and adopt a plan	$5,000	$10,000
Failure to fully implement plan	5,000	10,000
Inadequate plan	2,500	10,000
Roadway Signals and Cab Signals—		
236.21 Location of roadway signals	1,000	2,000
236.22 Semaphore signal arm; clearance to other objects	1,000	2,000

Section	Violation	Willful violation
236.23 Aspects and indications	1,000	2,000
236.24 Spacing of roadway signals	2,500	5,000
236.26 Buffing device, maintenance	1,000	2,000
Track Circuits—		
236.51 Track circuit requirements:		
(a) Shunt fouling circuit used where permissible speed through turnout greater than 45 m.p.h	2,500	5,000
(b) Track relay not in de-energized position or device that functions as track relay not in its most restrictive state when train, locomotive, or car occupies any part of track circuit, except fouling section of turnout of hand-operated main-track crossover	2,500	5,000
(c) other violations	1,000	2,000
236.52 Relayed cut-section	1,000	2,000
236.53 Track circuit feed at grade crossing	1,000	2,000
236.54 Minimum length of track circuit	1,000	2,000
236.55 Dead section; maximum length	1,000	2,000
236.56 Shunting sensitivity	2,500	5,000
236.57 Shunt and fouling wires:		
(a) Shunt or fouling wires do not consist of at least two discrete conductors	2,500	5,000
(b) other violations	1,000	2,000
236.58 Turnout, fouling section:		
(a) Rail joint in shunt fouling section not bonded	2,500	5,000
(b) other violations	1,000	2,000
236.59 Insulated rail joints	1,000	2,000
236.60 Switch shunting circuit; use restricted	2,500	5,000
Wires and Cables—		
236.71 Signal wires on pole line and aerial cable	1,000	2,000
236.73 Open-wire transmission line; clearance to other circuits	1,000	2,000
236.74 Protection of insulated wire; splice in underground wire	1,000	2,000
236.76 Tagging of wires and interference of wires or tags with signal apparatus	1,000	2,000
Inspections and Tests; All Systems—		
236.101 Purpose of inspection and tests; removal from service or relay or device failing to meet test requirements	2,500	5,000
236.102 Semaphore or search-light signal mechanism	1,000	2,000
236.103 Switch circuit controller or point detector	1,000	2,000
236.104 Shunt fouling circuit	1,000	2,000
236.105 Electric lock	1,000	2,000
236.106 Relays	1,000	2,000
236.107 Ground tests	1,000	2,000
236.108 Insulation resistance tests, wires in trunking and cables:		
(a) Circuit permitted to function on a conductor having insulation resistance value less than 200,000 ohms	2,500	5,000
(b) other violations	1,000	2,000
236.109 Time releases, timing relays and timing devices	1,000	2,000
236.110 Results of tests	1,000	2,000
Subpart B—Automatic Block Signal Systems		
236.201 Track circuit control of signals	1,000	2,000
236.202 Signal governing movements over hand-operated switch	1,000	2,000
236.203 Hand-operated crossover between main tracks; protection	1,000	2,000
236.204 Track signaled for movements in both directions, requirements	1,000	2,000
236.205 Signal control circuits; requirements	1,000	2,000
236.206 Battery or power supply with respect to relay; location	1,000	2,000
Subpart C—Interlocking		
236.207 Electric lock on hand-operated switch; control:		
(a) Approach or time locking of electric lock on hand-operated switch can be defeated by unauthorized use of emergency device which is not kept sealed in the non-release position	2,500	5,000
(b) other violations	1,000	2,000
236.301 Where signals shall be provided	1,000	2,000
236.302 Track circuits and route locking	1,000	2,000
236.303 Control circuits for signals, selection through circuit controller operated by switch points or by switch locking mechanism	1,000	2,000
236.304 Mechanical locking or same protection effected by circuits	1,000	2,000
236.305 Approach or time locking	1,000	2,000
236.306 Facing point lock or switch-and-lock movement	1,000	2,000
236.307 Indication locking:		
236.308 Mechanical or electric locking or electric circuits; requisites	1,000	2,000

Section	Violation	Willful violation
236.309 Loss of shunt protection; where required:		
(a) Loss of shunt of five seconds or less permits release of route locking of power-operated switch, movable point frog, or derail	2,500	5,000
(b) Other violations	1,000	2,000
236.310 Signal governing approach to home signal	1,000	2,000
236.311 Signal control circuits, selection through track relays or devices functioning as track relays and through signal mechanism contacts and time releases at automatic interlocking	1,000	2,000
236.312 Movable bridge, interlocking of signal appliances with bridge devices:		
(a) Emergency bypass switch or device not locked or sealed	2,500	5,000
(b) other violations	1,000	2,000
236.314 Electric lock for hand-operated switch or derail:		
(a) Approach or time locking of electric lock at hand-operated switch or derail can be defeated by unauthorized use of emergency device which is not kept sealed in non-release position	2,500	5,000
(b) other violations	1,000	2,000
Rules and Instructions—		
236.326 Mechanical locking removed or disarranged; requirement for permitting train movements through interlocking	1,000	2,000
236.327 Switch, movable-point frog or split-point derail	1,000	2,000
236.328 Plunger of facing-point	1,000	2,000
236.329 Bolt lock	1,000	2,000
236.330 Locking dog of switch and lock movement	1,000	2,000
236.334 Point detector	1,000	2,000
236.335 Dogs, stops and trunnions of mechanical locking	1,000	2,000
236.336 Locking bed	1,000	2,000
236.337 Locking faces of mechanical locking; fit	1,000	2,000
236.338 Mechanical locking required in accordance with locking sheet and dog chart	1,000	2,000
236.339 Mechanical locking; maintenance requirements	1,000	2,000
236.340 Electromechanical interlocking machine; locking between electrical and mechanical levers	1,000	2,000
236.341 Latch shoes, rocker links, and quadrants	1,000	2,000
236.342 Switch circuit controller	1,000	2,000
Inspection and Tests—		
236.376 Mechanical locking	1,000	2,000
236.377 Approach locking	1,000	2,000
236.378 Time locking	1,000	2,000
236.379 Route locking	1,000	2,000
236.380 Indication locking	1,000	2,000
236.381 Traffic locking	1,000	2,000
236.382 Switch obstruction test	1,000	2,000
236.383 Valve locks, valves, and valve magnets	1,000	2,000
236.384 Cross protection		
236.386 Restoring feature on power switches		
236.387 Movable bridge locking	1,000	2,000
Subpart D—Traffic Control Systems Standards		
236.401 Automatic block signal system and interlocking standards applicable to traffic control systems:		
236.402 Signals controlled by track circuits and control operator	1,000	2,000
236.403 Signals at controlled point	1,000	2,000
236.404 Signals at adjacent control points	1,000	2,000
236.405 Track signaled for movements in both directions, change of direction of traffic	1,000	2,000
236.407 Approach or time locking; where required	1,000	2,000
236.408 Route locking	1,000	2,000
236.410 Locking, hand-operated switch; requirements:		
(a) Hand-operated switch on main track not electrically or mechanically locked in normal position where signal not provided to govern movement to main track, movements made at speeds in excess of 20 m.p.h., and train or engine movements may clear main track	2,500	5,000
(b) Hand-operated switch on signaled siding not electrically or mechanically locked in normal position where signal not provided to govern movements to signaled siding, train movements made at speeds in excess of 30 m.p.h., and train or engine movements may clear signaled siding	2,500	5,000
(c) Approach or time locking of electric lock at hand-operated switch can be defeated by use of emergency release device of electric lock which is not kept sealed in non-release position	2,500	5,000
(d) other violations	1,000	2,000
Rules and Instructions—		
236.426 Interlocking rules and instructions applicable to traffic control systems	1,000	2,000
236.476 Interlocking inspections and tests applicable to traffic control systems	1,000	2,000

Section	Violation	Willful violation
Subpart E—Automatic Train Stop, Train Control and Cab Signal Systems Standards		
236.501 Forestalling device and speed control	1,000	2,000
236.502 Automatic brake application, initiation by restrictive block conditions stopping distance in advance	1,000	2,000
236.503 Automatic brake application; initiation when predetermined rate of speed exceeded	1,000	2,000
236.504 Operations interconnected with automatic block-signal system	1,000	2,000
236.505 Proper operative relation between parts along roadway and parts on locomotive	1,000	2,000
236.506 Release of brakes after automatic application	1,000	2,000
236.507 Brake application; full service	1,000	2,000
236.508 Interference with application of brakes by means of brake valve	1,000	2,000
236.509 Two or more locomotives coupled	1,000	2,000
236.511 Cab signals controlled in accordance with block conditions stopping distance in advance	1,000	2,000
236.512 Cab signal indication when locomotive enters blocks	1,000	2,000
236.513 Audible indicator	1,000	2,000
236.514 Interconnection of cab signal system with roadway signal system	1,000	2,000
236.515 Visibility of cab signals	1,000	2,000
236.516 Power supply	1,000	2,000
Rules and Instructions; Roadway—		
236.526 Roadway element not functioning properly	2,500	5,000
236.527 Roadway element insulation resistance	1,000	2,000
236.528 Restrictive condition resulting from open hand-operated switch; requirement	1,000	2,000
236.529 Roadway element inductor; height and distance from rail	1,000	2,000
236.531 Trip arm; height and distance from rail	1,000	2,000
236.532 Strap iron inductor; use restricted	1,000	2,000
236.534 Rate of pressure reduction; equalizing reservoir or brake pipe	1,000	2,000
236.551 Power supply voltage	1,000	2,000
236.552 Insulation resistance	1,000	2,000
236.553 Seal, where required	2,500	5,000
236.554 Rate of pressure reduction; equalizing reservoir or brake pipe	1,000	2,000
236.555 Repaired or rewound receiver coil	1,000	2,000
236.556 Adjustment of relay	1,000	2,000
236.557 Receiver; location with respect to rail	1,000	2,000
236.560 Contact element, mechanical trip type; location with respect to rail	1,000	2,000
236.562 Minimum rail current required	1,000	2,000
236.563 Delay time	1,000	2,000
236.564 Acknowledging time	1,000	2,000
236.565 Provision made for preventing operation of pneumatic brake-applying apparatus by double-heading clock; requirement	1,000	2,000
236.566 Locomotive of each train operating in train stop, train control or cab signal territory; equipped	5,000	7,500
236.567 Restrictions imposed when device fails and/or is cut out en route:		
(a) Report not made to designated officer at next available point of communication after automatic train stop, train control, or cab signal device fails and/or is cut en route	5,000	7,500
(b) Train permitted to proceed at speed exceeding 79 m.p.h. where automatic train stop, train control, or cab signal device fails and/or is cut out en route when absolute block established in advance of train on which device is inoperative	5,000	7,500
(c) other violations	1,000	2,000
236.568 Difference between speeds authorized by roadway signal and cab signal; action	1,000	2,000
Inspection and Tests; Roadway—		
236.576 Roadway element	1,000	2,000
236.577 Test, acknowledgement, and cut-in circuits	1,000	2,000
Inspection and Tests; Locomotive—		
236.586 Daily or after trip test	2,500	5,000
236.587 Departure test:		
(a) Test of automatic train stop, train control, or cab signal apparatus on locomotive not made on departure of locomotive from initial terminal if equipment on locomotive not cut out between initial terminal and equipped territory	5,000	7,500
(b) Test of automatic train stop, train control, or cab signal apparatus on locomotive not made immediately on entering equipped territory, if equipment on locomotive cut out between initial terminal and equipped territory	5,000	7,500
(c) Automatic train stop, train control, or cab signal apparatus on locomotive making more than one trip within 24-hour period not given departure test within corresponding 24-hour period	5,000	7,500
(d) other violations	2,500	5,000
236.588 Periodic test	2,500	5,000
236.589 Relays	2,500	5,000
236.590 Pneumatic apparatus:		
(a) Automatic train stop, train control, or cab signal apparatus not inspected and cleaned at least once every 736 days	2,500	5,000
(b) other violations	1,000	2,000

Section	Violation	Willful violation
Subpart F—Dragging Equipment and Slide Detectors and Other Similar Protective Devices; Standards		
236.601 Signals controlled by devices; location	1,000	2,000
Subpart H—Standards for Processor-Based Signal and Train Control Systems		
236.905 Railroad Safety Program Plan (RSPP):		
Failure to develop and submit RSPP when required	5,000	7,500
Failure to obtain FRA approval for a modification to RSPP	5,000	7,500
236.907 Product Safety Plan (PSP):		
Failure to develop a PSP	5,000	7,500
Failure to submit a PSP when required	5,000	7,500
236.909 Minimum Performance Standard:		
Failure to make analyses or documentation available	2,500	5,000
Failure to determine that the standard has been met	5,000	7,500
236.913 Notification to FRA of PSPs:	2,500	5,000
Failure to prepare a PSP or PSP amendment as required	5,000	7,500
Failure to submit a PSP or PSP amendment as required	5,000	7,500
Field testing without authorization or approval	10,000	20,000
236.915 Implementation and operation:		
(a) Operation of product without authorization or approval	10,000	20,000
(b) Failure to comply with PSP	2,500	5,000
(c) Interference with normal functioning safety-critical product	7,500	15,000
(d) Failure to determine cause and adjust, repair or replace without undue delay or take appropriate action pending repair	5,000	7,500
236.917 Retention of records:		
Failure to maintain records as required	7,500	15,000
Failure to report inconsistency	10,000	20,000
Failure to take prompt countermeasures	10,000	20,000
Failure to provide final report	2,500	5,000
236.919 Operations and Maintenance Manual	3,000	6,000
236.921 Training and qualification program, general	3,000	6,000
236.923 Task analysis and basic requirements:		
Failure to develop an acceptable training program	2,500	5,000
Failure to train persons as required	2,500	5,000
Failure to conduct evaluation of training program as required	2,500	5,000
Failure to maintain records as required	1,500	3,000
236.925 Training specific to control office personnel	2,500	5,000
236.927 Training specific to locomotive engineers and other operating personnel	2,500	5,000
236.929 Training specific to roadway workers	2,500	5,000
Subpart I—Positive Train Control Systems		
236.1005 Positive Train Control System Requirements:		
Failure to timely complete PTC system installation on track segment where PTC is required	16,000	25,000
Commencement of revenue service prior to obtaining PTC System Certification	16,000	25,000
Failure of the PTC system to perform a safety-critical function required by this section	5,000	7,500
Operating outside the limits of an approved *de minimis* exception	15,000	25,000
Failure to integrate a hazard detector	15,000	25,000
Non-compliant event recorder	2,500	5,000
Failure of event recorder	2,500	5,000
Failure to provide notice, obtain approval, or follow a condition for temporary rerouting when required	5,000	7,500
Exceeding the allowed percentage of controlling locomotives operating out of an initial terminal after receiving a failed initialization	5,000	7,500
236.1006 Equipping locomotives operating in PTC territory:		
Failure to adhere to a PTCIP.	[2]	[2]
Operating in PTC territory a controlling locomotive without a required and operative PTC onboard apparatus	15,000	25,000
Operating with a PTC onboard apparatus that is not functioning in accordance with the applicable PTCSP..	15,000	25,000
Failure to report as prescribed by this section	5,000	7,500
Non-compliant operation of unequipped trains in PTC territory	15,000	25,000
Failure to equip locomotives in accordance with the applicable PTCIP	15,000	25,000
Failure to comply with conditions of a yard movement exception	[2]	[2]
Improper arrangement of the PTC system onboard apparatus	2,500	5,000
Engineer performing prohibited duties	5,000	7,500
236.1007 Additional requirements for high-speed service:		
Installing or operating a PTC system without the required safety-critical functional attributes of a block signal system	15,000	25,000
Operation of passenger trains at speed equal to or greater than 60 mph on non-PTC-equipped territory where required	15,000	25,000
Operation of freight trains at speed equal to or greater than 50 mph on non-PTC-equipped territory where required	15,000	25,000

Section	Violation	Willful violation
Failure to fully implement incursion protection where required	5,000	7,500
236.1009 Procedural requirements:		
Failure to file PTCIP when required	5,000	7,500
Failure to amend PTCIP when required	5,000	7,500
Failure to obtain Type Approval when required	5,000	7,500
Failure to update NPI	5,000	7,500
Operation of PTC system without system certification	16,000	25,000
Failure to comply with FRA condition or modification	(2)	(2)
Failure to report as required	5,000	7,500
Failure to provide FRA access	10,000	16,000
236.1011 PTCIP content requirements:		
Failure to install a PTC system as required	11,000	16,000
Failure to maintain a PTCIP as required	(2)	(2)
236.1013 PTCDP content requirements and Type Approval:		
Failure to maintain quality control system	5,000	7,500
Inappropriate use of Type Approval	5,000	7,500
236.1015 PTCSP content requirements and PTC System Certification:		
Failure to implement PTC system in accordance with the associated PTCSP and resultant system certification	16,000	25,000
Failure to maintain PTC system in accordance with the associated PTCSP and resultant system certification	16,000	25,000
Failure to maintain required supporting documentation	2,500	5,000
236.1017 Independent third party Verification and Validation:		
Failure to conduct independent third party Verification and Validation when ordered	11,000	16,000
236.1019 Main line track exceptions:		
Operations conducted in non-compliance with the passenger terminal exception	16,000	25,000
Operations conducted in non-compliance with the limited operations exception	16,000	25,000
Failure to request modification of the PTCIP or PTCSP when required	11,000	16,000
Operations conducted in violation of (c)(2)	16,000	25,000
Operations conducted in violation of (c)(3)	25,000	25,000
236.1021 Discontinuances, material modifications, and amendments:		
Failure to update PTCDP when required	5,000	7,500
Failure to update PTCSP when required	5,000	7,500
Failure to immediately adopt and comply with approved RFA	5,000	7,500
Discontinuance or modification of a PTC system without approval when required	11,000	16,000
236.1023 Errors and malfunctions:		
Railroad failure to provide proper notification of PTC system error or malfunction	5,000	7,500
Failure to maintain PTCPVL	2,500	5,000
Supplier failure to provide proper notification of previously identified PTC system error or malfunction	5,000	7,500
Failure to provide timely notification	5,000	7,500
Failure to provide appropriate protective measures in the event of PTC system failure	15,000	25,000
236.1027 Exclusions:		
Integration of primary train control system with locomotive electronic system without approval	5,000	7,500
236.1029 PTC system use and en route failures:		
Failure to determine cause of PTC system component failure without undue delay	5,000	7,500
Failure to adjust, repair, or replace faulty PTC system component without undue delay	5,000	7,500
Failure to take appropriate action pending adjustment, repair, or replacement of faulty PTC system component	15,000	25,000
PTC territory operation with an inoperative PTC onboard apparatus	5,000	7,500
Interference with the normal functioning of safety-critical PTC system	15,000	25,000
236.1033 Communications and security requirements:		
Failure to provide cryptographic message integrity and authentication	5,000	7,500
Improper use of revoked cryptographic key	5,000	15,000
Failure to protect cryptographic keys from unauthorized disclosure, modification, or substitution	5,000	15,000
Failure to establish prioritized service restoration and mitigation plan for communication services	5,000	7,500
236.1035 Field testing requirements:		
Field testing without authorization or approval	10,000	20,000
Failure to comply with FRA condition	(2)	(2)
236.1037 Records retention:		
Failure to maintain records and databases as required	7,500	15,000
Failure to report inconsistency	10,000	20,000
Failure to take prompt countermeasures	10,000	20,000
Failure to provide final report	2,500	5,000
236.1039 Operations and Maintenance Manual:		
Failure to implement and maintain Operations and Maintenance Manual as required	3,000	6,000
Failure to make Operations and Maintenance Manual available to FRA when required	10,000	16,000
Failure to make Operations and Maintenance Manual available to persons required to performed the required tasks	15,000	25,000
Amends Operations and Maintenance Manual without FRA approval	5,000	10,000

Section	Violation	Willful violation
236.1043 Task analysis and basic requirements:		
Failure to develop and maintain an acceptable training program	10,000	20,000
Failure to train persons as required	2,500	5,000
Failure to conduct evaluation of training program as required	2,500	5,000
Failure to maintain records as required	1,500	3,000
236.1045 Training specific to office control personnel:		
Failure to conduct training unique to office control personnel	2,500	5,000
236.1047 Training specific to locomotive engineers and other operating personnel:		
Failure to conduct training unique to locomotive engineers and other operating personnel	2,500	5,000
236.1049 Training specific to roadway workers:		
Failure to conduct training unique to roadway workers	2,500	5,000

[1] A penalty may be assessed against an individual only for a willful violation. The Administrator reserves the right to assess a civil penalty of up to $109,819 per day for any violation where circumstances warrant. See 49 CFR part 209, Appendix A.

[2] Each plan has numerous conditions and requirements with varying degrees of importance or impact. Thus, a single recommended civil penalty amount for a violation for failure to adhere to each plan or condition is not advisable or warranted. When a violation of a plan or condition is found, FRA may consider a variety of factors to determine the appropriate civil penalty to assess, including any underlying or related violation.

[53 FR 52936, Dec. 29, 1988, as amended at 63 FR 11624, Mar. 10, 1998; 69 FR 30595, May 28, 2004; 70 FR 11104, Mar. 7, 2005; 73 FR 79704, Dec. 30, 2008; 75 FR 2715, Jan. 15, 2010; 77 FR 24422, Apr. 24, 2012; 81 FR 10129, Feb. 29, 2016; 81 FR 43112, July 1, 2016]

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 minimum 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 control system that operates over the designated life-cycle of the product. 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 risk assessment of each safety-critical system (product) must account not only for the risks associated with each subsystem or component, but also for the risks associated with interactions (interfaces) between such subsystems.

(c) *What is the main principle in computing risk for the previous and current conditions?* The risk for the previous condition must be computed using the same metrics as for the new system being proposed. A full risk assessment must consider the entire railroad environment where the product is being applied, and show all aspects of the previous condition that are affected by the installation of the product, considering all faults, operating errors, exposure scenarios, and consequences that are related as described in this part. For the full risk assessment, the total societal cost of the potential numbers of accidents assessed for both previous and new system conditions must be computed for comparison. An abbreviated risk assessment must, as a minimum, clearly compute the MTTHE for all of the hazardous events identified for both previous and current conditions. The comparison between MTTHE for both conditions is to determine whether the product implementation meets the safety criteria as required by subpart H or subpart I of this part as applicable.

(d) *What major system characteristics must be included when relevant to risk 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, switches, rail crossings at grade and highway-rail grade crossings as applicable;

(2) Train movement density for freight, work, and passenger trains where applicable and computed over a time span of not less than 12 months;

(3) Train movement operational rules, as enforced by the dispatcher, roadway worker/Employee in Charge, and train crew behaviors;

(4) Wayside subsystems and components;

(5) Onboard subsystems and components;

(6) Consist contents such as hazardous material, oversize loads; and

(7) Operating speeds if the provisions of part 236 cite additional requirements for certain type of train control systems to be used at such speeds for freight and passenger trains.

(e) *What other relevant parameters must be determined for the subsystems and components?*

In order to derive the frequency of hazardous events (or MTTHE) applicable for a product, subsystem or component included in the risk assessment, the railroad may use various techniques, such as reliability and availability calculations for subsystems and components, Fault Tree Analysis (FTA) of the subsystems, and results of the application of safety design principles as noted in Appendix C to this part. The MTTHE is to be derived for both fail-safe and non-fail-safe subsystems or components. The lower bounds of the MTTF or MTBF determined from the system sensitivity analysis, which account for all necessary and well justified assumptions, may be used to represent the estimate of MTTHE for the associated non-fail-safe subsystem or component in the risk assessment.

(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 the 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) Software fault/failure analysis must be based on the assessment of the design and implementation of all safety-related software including the application code, its operating/executive program, COTS software, and associated device drivers, as well as historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The software assessment process must demonstrate through repeatable predictive results that all software defects have been identified and corrected by process with 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 operation after 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 adequacy by a documented 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 for risk assessment?* (1) The railroad shall document any assumptions regarding the derivation of risk metrics used. For example, for the full risk assessment, all assumptions made about each value of the parameters used in the calculation of total cost of accidents should be documented. For abbreviated risk assessment, all assumptions made for MTHHE derivation using existing reliability and availability data on the current system components should be documented. The railroad shall document these assumptions in such a form as to permit later comparisons with in-service experience.

(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 that permit 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 comparisons with in-service experience.

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

[75 FR 2717, Jan. 15, 2010]

APPENDIX C TO PART 236—SAFETY ASSURANCE CRITERIA AND PROCESSES

(a) *What is the purpose of this appendix?* This appendix provides safety criteria and processes that the designer must use to develop and validate the product that meets safety requirements of this part. FRA uses the criteria and processes set forth in this appendix to evaluate the validity of safety targets and the results of system safety analyses provided in the RSPP, PSP, PTCIP, PTCDP, and PTCSP documents as appropriate. An analysis performed under this appendix must:

(1) Address each of the safety principles of paragraph (b) of this appendix, or explain why they are not relevant, and

(2) Employ a validation and verification process pursuant to paragraph (c) of this appendix.

(b) *What safety principles must be followed during product development?* The designer shall address each of the following safety considerations principles when designing and demonstrating the safety of products covered

by subpart H or I of this part. In the event that any of these principles are not followed, the PSP or PTCDP or PTCSP 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) *System safety under normal operating conditions.* The system (all its elements including hardware and software) must be designed to assure safe operation with no hazardous events 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. The system shall operate safely even in the absence of prescribed operator actions or procedures. The designer must identify and categorize all hazards that may lead to unsafe system operation. Hazards categorized as unacceptable, which are determined by hazard analysis, must be eliminated by design. Best effort shall also be made by the designer to eliminate by design the hazards categorized as undesirable. Those undesirable hazards that cannot be eliminated should be mitigated to the acceptable level as required by this part.

(2) *System safety under failures.*

(i) It must be shown how the product is designed to eliminate or mitigate 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; 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.

(ii) The product must be shown to operate safely under conditions of random hardware failures. This includes single hardware failures as well as multiple hardware failures that may occur at different times but 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).

(iii) 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 that eliminates the possibility of false activation of any physical appliance.

(iv) 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 that eliminates the possibility of false activation of any physical appliance.

(v) Another concern of multiple failures 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.

(3) *Closed loop principle.* System design adhering to the closed loop principle requires that all conditions necessary for the existence of any permissive state or action be verified to be present before the permissive state or action can be initiated. Likewise the requisite conditions shall be verified to be continuously present for the permissive state or action to be maintained. This is in contrast to allowing a permissive state or action to be initiated or maintained in the absence of detected failures. In addition, closed loop design requires that failure to perform a logical operation, or absence of a logical input, output or decision shall not cause an unsafe condition, i.e. system safety does not depend upon the occurrence of an action or logical decision.

(4) *Safety assurance concepts.* The product design must include one or more of the following Safety Assurance Concepts as described in IEEE–1483 standard to ensure that failures are detected and the product is placed in a safe state. One or more different principles may be applied to each individual subsystem or component, depending on the safety design objectives of that part of the product.

(i) *Design diversity and self-checking concept.* This concept requires that all critical functions be performed in diverse ways, using diverse software operations and/or diverse

hardware channels, and that critical hardware be tested with Self-Checking routines. Permissive outputs are allowed only if the results of the diverse operations correspond, and the Self-Checking process reveals no failures in either execution of software or in any monitored input or output hardware. If the diverse operations do not agree or if the checking reveals critical failures, safety-critical functions and outputs must default to a known safe state.

(ii) *Checked redundancy concept.* The Checked Redundancy concept requires implementation of two or more identical, independent hardware units, each executing identical software and performing identical functions. A means is to be provided to periodically compare vital parameters and results of the independent redundant units, requiring agreement of all compared parameters to assert or maintain a permissive output. If the units do not agree, safety-critical functions and outputs must default to a known safe state.

(iii) *N-version programming concept.* This concept requires a processor-based product to use at least two software programs performing identical functions and executing concurrently in a cycle. The software programs must be written by independent teams, using different tools. The multiple independently written software programs comprise a redundant system, and may be executed either on separate hardware units (which may or may not be identical) or within one hardware unit. A means is to be provided to compare the results and output states of the multiple redundant software systems. If the system results do not agree, then the safety-critical functions and outputs must default to a known safe state.

(iv) *Numerical assurance concept.* This concept requires that the state of each vital parameter of the product or system be uniquely represented by a large encoded numerical value, such that permissive results are calculated by pseudo-randomly combining the representative numerical values of each of the critical constituent parameters of a permissive decision. Vital algorithms must be entirely represented by data structures containing numerical values with verified characteristics, and no vital decisions are to be made in the executing software, only by the numerical representations themselves. In the event of critical failures, the safety-critical functions and outputs must default to a known safe state.

(v) *Intrinsic fail-safe design concept.* Intrinsically fail-safe hardware circuits or systems are those that employ discrete mechanical and/or electrical components. The fail-safe operation for a product or subsystem designed using this principle concept requires a verification that the effect of every relevant failure mode of each component, and relevant combinations of component failure modes, be considered, analyzed, and documented. This is typically performed by a comprehensive failure modes and effects analysis (FMEA) which must show no residual unmitigated failures. In the event of critical failures, the safety-critical functions and outputs must default to a known safe state.

(5) *Human factor engineering principle.* 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.

(6) *System safety under 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.

(7) *System safety after 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. Such modifications must follow all of the concept, design, implementation and test processes and principles as documented in the PSP for the original product. Regression testing must be comprehensive and documented to include all scenarios which are affected by the change made, and the operating modes of the changed product during normal and failure state (fallback) operation.

(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 and subpart I 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 and subpart I

of this part. The latest versions of the standards listed below should be used unless otherwise provided.

(i) IEEE standards as follows:

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

(B) IEEE 1474.2–2003, Standard for user interface requirements in communications based train control (CBTC) systems.

(C) IEEE 1474.1–2004, Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements.

(ii) CENELEC Standards as follows:

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

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

(iii) ATCS Specification 200 Communications Systems Architecture.

(iv) ATCS Specification 250 Message Formats.

(v) AREMA 2009 Communications and Signal Manual of Recommended Practices, Part 16, Part 17, 21, and 23.

(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—Part 3: 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.

(H) IEC 62278: 2002, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(I) IEC 62279: 2002 Railway Applications: Software for Railway Control and Protection Systems;

(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.

(5) The various standards provided in this paragraph are for illustrative purposes only. Copies of these standards can be obtained in accordance with the following:

(i) U.S. government standards and technical publications may be obtained by contacting the federal National Technical Information Service, 5301 Shawnee Rd, Alexandria, VA 22312.

(ii) U.S. National Standards may be obtained by contacting the American National Standards Institute, 25 West 43rd Street, 4 Floor, New York, NY 10036.

(iii) IEC Standards may be obtained by contacting the International Electrotechnical Commission, 3, rue de Varembé, P.O. Box 131 CH—1211, GENEVA, 20, Switzerland.

(iv) CENLEC Standards may be obtained by contacting any of one the national standards bodies that make up the European Committee for Electrotechnical Standardization.

(v) IEEE standards may be obtained by contacting the IEEE Publications Office, 10662 Los Vaqueros Circle, P.O. Box 3014, Los Alamitos, CA 90720–1264.

(vi) AREMA standards may be obtained from the American Railway Engineering and Maintenance-of-Way Association, 10003 Derekwood Lane, Suite 210, Lanham, MD 20706.

[75 FR 2718, Jan. 15, 2010]

APPENDIX D TO PART 236—INDEPENDENT REVIEW OF VERIFICATION AND VALIDATION

(a) This appendix provides minimum requirements for independent third-party assessment of product safety verification and validation pursuant to subpart H or subpart I 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 any mutually agreed upon controlling documents and standards and the applicable railroad's:

(1) Railroad Safety Program Plan (RSPP) and Product Safety Plan (PSP) for processor based systems developed under subpart H or,

(2) PTC Product Development Plan (PTCDP) and PTC Safety Plan (PTCSP) for PTC systems developed under subpart I.

(b) 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 shall not engage in any design efforts associated with the product, the products subsystems, or the products components, in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the product.

(c) 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.

(d) The reviewer shall evaluate the product 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 validation and verification 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 and document the adequacy of the railroad's

(1) RSPP, the PSP, and any other documents pertinent to a product being developed under subpart H of this part; or

(2) PTCDP and PTCSP for systems being developed under subpart I of this part.

(e) The reviewer shall analyze the Hazard Log and/or any other hazard analysis documents for comprehensiveness and compliance with applicable railroad, vendor, supplier, industry, national, and international standards.

(f) 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 applicable railroad, vendor, supplier, industry, national and international standards.

(g) The reviewer shall randomly select various safety-critical software, and hardware modules, if directed by FRA, for audit to verify whether the requirements of the applicable railroad, vendor, supplier, industry, national, and international standards 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 applicable railroad, vendor, supplier, industry, national, and international standards.

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

(i) 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:

(1) Reviewer's evaluation of the adequacy of the PSP in the case of products developed under subpart H, or PTCSP for products developed under subpart I of this part, including the supplier's MTTHE and risk estimates for the product, and the supplier's confidence interval in these estimates;

(2) Product vulnerabilities, potentially hazardous failure modes, or potentially hazardous operating circumstances which the reviewer felt were not adequately identified, tracked, mitigated, and corrected by either the vendor or supplier or the railroad;

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

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

(5) A listing of each applicable vendor, supplier, industry, national, or international standard, procedure or process which was not properly followed;

(6) Identification of the software verification and validation procedures, as well as the hardware verification validation procedures if deemed appropriate by FRA, for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(7) Methods employed by the product manufacturer to develop safety-critical software;

(8) If deemed applicable by FRA, the methods employed by the product manufacturer to develop safety-critical hardware by generally acceptable techniques;

(9) 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.

[75 FR 2720, Jan. 15, 2010]

APPENDIX E TO PART 236—HUMAN-MACHINE INTERFACE (HMI) DESIGN

(a) This appendix provides human factors design criteria applicable to both subpart H and subpart I of this part. HMI design criteria will minimize negative safety effects by causing designers to consider human factors in the development of HMIs. The product design should sufficiently incorporate

human factors engineering that is appropriate to the complexity of the product; the gender, 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.

(b) As used in this section, ''designer'' means anyone who specifies requirements for—or designs a system or subsystem, or both, for—a product subject to subpart H or subpart I of this part, and ''operator'' means any human who is intended to receive information from, provide information to, or perform repairs or maintenance on a safety-critical product subject to subpart H or I of this part.

(c) Human factors issues the designers must consider with regard to the general function of a system include:

(1) *Reduced situational awareness and over-reliance.* HMI design must give an operator active functions to perform, feedback on the results of the operator's actions, and information on the automatic functions of the system as well as its performance. The operator must be ''in-the-loop.'' Designers must consider at a minimum the following methods of maintaining an active role for human operators:

(i) The system must require an operator to initiate action to operate the train and require an operator to remain ''in-the-loop'' for at least 30 minutes at a time;

(ii) The system must provide timely feedback to an operator regarding the system's automated actions, the reasons for such actions, and the effects of the operator's manual actions on the system;

(iii) The system must warn operators in advance when it requires an operator to take action;

(iv) HMI design must equalize an operator's workload; and

(v) HMI design must not distract from the operator's safety related duties.

(2) *Expectation of predictability and consistency in product behavior and communications.* HMI design must accommodate an operator's expectation of logical and consistent relationships between actions and results. Similar objects must behave consistently when an operator performs the same action upon them.

(3) *End user limited ability to process information.* HMI design must therefore minimize an operator's information processing load. To minimize information processing load, the designer must:

(i) Present integrated information that directly supports the variety and types of decisions that an operator makes;

(ii) Provide information in a format or representation that minimizes the time required to understand and act; and

(iii) Conduct utility tests of decision aids to establish clear benefits such as processing time saved or improved quality of decisions.

(4) *End user limited memory.* HMI design must therefore minimize an operator's information processing load.

(i) To minimize short-term memory load, the designer shall integrate data or information from multiple sources into a single format or representation (''chunking'') and design so that three or fewer ''chunks'' of information need to be remembered at any one time.

(ii) To minimize long-term memory load, the designer shall design to support recognition memory, design memory aids to minimize the amount of information that must be recalled from unaided memory when making critical decisions, and promote active processing of the information.

(d) Design systems that anticipate possible user errors and include capabilities to catch errors before they propagate through the system;

(1) Conduct cognitive task analyses prior to designing the system to better understand the information processing requirements of operators when making critical decisions; and

(2) Present information that accurately represents or predicts system states.

(e) When creating displays and controls, the designer must consider user ergonomics and shall:

(1) Locate displays as close as possible to the controls that affect them;

(2) Locate displays and controls based on an operator's position;

(3) Arrange controls to minimize the need for the operator to change position;

(4) Arrange controls according to their expected order of use;

(5) Group similar controls together;

(6) Design for high stimulus-response compatibility (geometric and conceptual);

(7) Design safety-critical controls to require more than one positive action to activate (e.g., auto stick shift requires two movements to go into reverse);

(8) Design controls to allow easy recovery from error; and

(9) Design display and controls to reflect specific gender and physical limitations of the intended operators.

(f) The designer shall also address information management. To that end, HMI design shall:

(1) Display information in a manner which emphasizes its relative importance;

(2) Comply with the ANSI/HFS 100–1988 standard;

(3) Utilize a display luminance that has a difference of at least 35cd/m2 between the foreground and background (the displays should be capable of a minimum contrast 3:1 with 7:1 preferred, and controls should be

provided to adjust the brightness level and contrast level);

(4) Display only the information necessary to the user;

(5) Where text is needed, use short, simple sentences or phrases with wording that an operator will understand and appropriate to the educational and cognitive capabilities of the intended operator;

(6) Use complete words where possible; where abbreviations are necessary, choose a commonly accepted abbreviation or consistent method and select commonly used terms and words that the operator will understand;

(7) Adopt a consistent format for all display screens by placing each design element in a consistent and specified location;

(8) Display critical information in the center of the operator's field of view by placing items that need to be found quickly in the upper left hand corner and items which are not time-critical in the lower right hand corner of the field of view;

(9) Group items that belong together;

(10) Design all visual displays to meet human performance criteria under monochrome conditions and add color only if it will help the user in performing a task, and use color coding as a redundant coding technique;

(11) Limit the number of colors over a group of displays to no more than seven;

(12) Design warnings to match the level of risk or danger with the alerting nature of the signal; and

(13) With respect to information entry, avoid full QWERTY keyboards for data entry.

(g) With respect to problem management, the HMI designer shall ensure that the:

(1) HMI design must enhance an operator's situation awareness;

(2) HMI design must support response selection and scheduling; and

(3) HMI design must support contingency planning.

(h) Ensure that electronics equipment radio frequency emissions are compliant with appropriate Federal Communications Commission regulations. The FCC rules and regulations are codified in Title 47 of the Code of Federal Regulations (CFR).

(1) Electronics equipment must have appropriate FCC Equipment Authorizations. The following documentation is applicable to obtaining FCC Equipment Authorization:

(i) OET Bulletin Number 61 (October, 1992 Supersedes May, 1987 issue) FCC Equipment Authorization Program for Radio Frequency Devices. This document provides an overview of the equipment authorization program to control radio interference from radio transmitters and certain other electronic products and an overview of how to obtain an equipment authorization.

(ii) OET Bulletin 63: (October 1993) Understanding The FCC Part 15 Regulations for Low Power, Non-Licensed Transmitters. This document provides a basic understanding of the FCC regulations for low power, unlicensed transmitters, and includes answers to some commonly-asked questions. This edition of the bulletin does not contain information concerning personal communication services (PCS) transmitters operating under Part 15, Subpart D of the rules.

(iii) 47 Code of Federal Regulations Parts 0 to 19. The FCC rules and regulations governing PCS transmitters may be found in 47 CFR, Parts 0 to 19.

(iv) OET Bulletin 62 (December 1993) Understanding The FCC Regulations for Computers and other Digital Devices. This document has been prepared to provide a basic understanding of the FCC regulations for digital (computing) devices, and includes answers to some commonly-asked questions.

(2) Designers must comply with FCC requirements for Maximum Permissible Exposure limits for field strength and power density for the transmitters operating at frequencies of 300 kHz to 100 GHz and specific absorption rate (SAR) limits for devices operating within close proximity to the body. The Commission's requirements are detailed in parts 1 and 2 of the FCC's Rules and Regulations (47 CFR 1.1307(b), 1.1310, 2.1091, 2.1093). The following documentation is applicable to demonstrating whether proposed or existing transmitting facilities, operations or devices comply with limits for human exposure to radiofrequency RF fields adopted by the FCC:

(i) OET Bulletin No. 65 (Edition 97–01, August 1997), ''Evaluating Compliance With FCC Guidelines For Human Exposure To Radiofrequency Electromagnetic Fields'',

(ii) OET Bulletin No 65 Supplement A, (Edition 97–01, August 1997), OET Bulletin No 65 Supplement B (Edition 97–01, August 1997) and

(iii) OET Bulletin No 65 Supplement C (Edition 01–01, June 2001).

(3) The bulletin and supplements offer guidelines and suggestions for evaluating compliance. However, they are not intended to establish mandatory procedures. Other methods and procedures may be acceptable if based on sound engineering practice.

[75 FR 2720, Feb. 15, 2010]

Appendix F to Part 236—Minimum Requirements of FRA Directed Independent Third-Party Assessment of PTC System Safety Verification and Validation

(a) This appendix provides minimum requirements for mandatory independent third-party assessment of PTC system safety

verification and validation pursuant to subpart H or I of this part. The goal of this assessment is to provide an independent evaluation of the PTC system manufacturer's utilization of safety design practices during the PTC system's development and testing phases, as required by the applicable PSP, PTCDP, and PTCSP, the applicable requirements of subpart H or I of this part, and any other previously agreed-upon controlling documents or standards.

(b) The supplier may request advice and assistance of the independent third-party 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 PTC system.

(c) 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.

(d) 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 PTC system. At a minimum, the reviewer shall evaluate the supplier design and development process regarding the use of an appropriate design methodology. The reviewer may use the comparison processes and test procedures that have been previously agreed to 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 applicable PSP or PTCSP, and any other documents pertinent to the PTC system being assessed.

(e) The reviewer shall analyze the Hazard Log and/or any other hazard analysis documents for comprehensiveness and compliance with railroad, vendor, supplier, industry, national, or international standards.

(f) 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 railroad, vendor, supplier, industry, national, or international standards.

(g) The reviewer shall randomly select various safety-critical software modules, as well as safety-critical hardware components if required by FRA for audit to verify whether the railroad, vendor, supplier, industry, national, or international standards 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 railroad, vendor, supplier, industry, national, or international standards

(h) The reviewer shall evaluate and comment on the plan for installation and test procedures of the PTC system for revenue service.

(i) 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:

(1) Reviewer's evaluation of the adequacy of the PSP or PTCSP including the supplier's MTTHE and risk estimates for the PTC system, and the supplier's confidence interval in these estimates;

(2) PTC system vulnerabilities, potentially hazardous failure modes, or potentially hazardous operating circumstances which the reviewer felt were not adequately identified, tracked or mitigated;

(3) A clear statement of position for all parties involved for each PTC system vulnerability cited by the reviewer;

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

(5) A listing of each applicable vendor, supplier, industry, national or international standard, process, or procedure which was not properly followed;

(6) Identification of the hardware and software verification and validation procedures for the PTC system's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(7) Methods employed by PTC system manufacturer to develop safety-critical software; and

(8) If directed by FRA, methods employed by PTC system manufacturer to develop safety-critical hardware.

[75 FR 2721, Jan. 15, 2010]

PART 237—BRIDGE SAFETY STANDARDS

Subpart A—General

Sec.

Subpart B—Railroad Bridge Safety Assurance