**Revised DP Text- 9/1/2009**

Relocated NIP Related Process Text from Section 1013 to Section 1009

Changed "Mechanisms" to "Components" Section 1011

Various Minor Editorial Changes (Renumbering, Grammar) & Accepted Text with no Comments from Morning Session

**PTCWG09-08-31,01,02-01 WG CONSENSUS**

**§ 236.1003 Definitions.**

*NPI* means a Notice of Product Intent ("NPI") as further described in § 236.1013

**Comment [MH1]:** Other definitions deleted to reduce amount of paper. No changes to those definitions

**§ 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 a 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; 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) If the host railroad is a freight railroad, and the subject trackage would require installation and operation of a PTC system in accordance with §§ 236.1005(b)(2) or (b)(3), then a PTCIP required to be filed in accordance with this paragraph (a)(1) or (a)(2) of this section must be jointly filed with each entity providing regularly scheduled intercity or commuter rail passenger transportation over that subject trackage. If railroads are unable to jointly file a PTCIP in accordance with paragraphs (a)(1) and (a)(3) of this section, then they each 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.

(b) Type Approval. A host railroad, or one or more system suppliers and one or more host railroads, 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 a NPI describing the functions of the proposed product. If a railroad elects to file a 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 for Safety, the Associate Administrator may grant "Provisional Approval" of the PTCIP.

(i) A "Provisional Approval" of a PTCIP is valid for a period of 9 months from the date of approval by the Associate Administrator for Safety.

(ii) 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 nine months of "Provisional Approval".

(A) Within 90 days of receipt of an updated PTCIP that was submitted with a NPI, the Associate Administrator will approve or disapprove of the updated PTCIP and notify in writing the affected railroad or other entity. 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§ 236.1009 and paragraph (a) of this section, as applicable.

(B) If an updated PTCIP to a "Provisionally Approved" PTCIP is not received by the Associate Administrator for Safety by the end of the ninth month, the "Provisional Approval" given to the PTCIP is automatically revoked. The revocation is retroactive to the date the original PTCIP and NPI was first submitted to the Associate Administrator for Safety.

**Comment [MH2]:** This paragraph was previously located in 1013(e)(2) and moved to this location. This location is more appropriately placed within section 1009 (Procedural) There was no change in the text.

(c) 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).

(d) 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.

(e) 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.

(f) 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;

(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.

(g) 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.

(h) 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.

**§ 236.1011 PTCIP 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);

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

(i) Include copies of relevant provisions of any 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 line segments will be equipped and the basis for those decisions, and shall at a minimum address the following risk factors by line 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

**Comment [MH3]:** Changed from "mechanisms" as discussed

**Formatted:** Line spacing: single

(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 December 31, 2015; and

(iii) 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 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)(iii)(A) of this section;

(7) The number of wayside devices required for each line segment and the installation schedule to complete wayside equipment installation by December 31, 2015;

(8) which track segments the railroad considers mainline and non-mainline track. If the PTCIP includes a 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; and

(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

(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 than 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 December 31, 2015.

(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.

(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.

**§ 236.1013 PTCDP 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, 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-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 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), 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;

(11) A description of the deviation required under § 236.1029(c), if applicable; and

(12) A complete description of how the PTC system will appropriate 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, a NPI must contain the following information:

(i) 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, track characteristics, and railroad operating rules;

(ii) 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;

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

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

(v) 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.

**Comment [MH4]:** The previous statement (e) "A railroad may…" moved to section 1009 Procedural Requirements. Sentence (e) revised to read "if submitted.

Letters (i) through (v) no change from previous text presented.

**§ 236.1015 PTCSP 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; and

(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 and

(3) Provides the applicable licensing information.

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

(1) Indicate the governing FRA approved PTCIP and, if applicable, the PTCDP and 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 PTCSP from that as described in the PTCDP, 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, 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 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 § 236.1033);

(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 § 236.1011(a)(10);

(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(e), if applicable;

(17) A description of the deviation required 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 appropriate 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)-(k); and

(20) Any alternative arrangements for each rail at-grade crossing not adhering to the table under § 236.1005(a)(1)(i).

(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 is 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 to otherwise intend to replace or materially modify the existing method of operation, shall:

(i) Demonstrate to reliably execute the functions required by § 236.1005; 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 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.

**PTCWG09-08-31,01,02,-03 WG CONSENSUS for Passenger TF recommendations**

**add a new subsection 236.1019(c)(4) as follows:**

**(4) passenger service is operated on a segment of track on which less than 5,000,000 gross tons of freight traffic is transported annually, and on which one of the following applies:**

**(a) if the segment is unsignaled (i.e., "dark territory"), no more than 4 regularly scheduled passenger trains are operated during a calendar day on which the maximum permitted speed for passenger trains is not greater than 59 miles per hour, or**

**(Consider "Switch Point Monitoring System and Track Integrity Warning System to be required)**

**(b) if the segment is signaled (e.g., equipped with CTC or ABS), no more than 12 regularly scheduled passenger trains on which the maximum permitted speed for passenger trains is not greater than 79 miles per hour, are operated during a calendar day.**

Comments:

Concerns over the use of the term "dark territory ". FRA to add clarity when refining language referring to CFR236.1005(e)(1)(i) to clarify intent & U.S.C.20164 (b).

State Mgrs. Object to approach and prefer this exception not be used, however, will vote they "can live with it"

**PTCWG09-08-31,01,02-02 WG CONSENSUS**

**§ 236.909 Minimum Performance Standard**

FRA is modifying existing § 236.909 to include a requirement for the risk metric sensitivity analysis to be an inherent part of the full risk assessment that is to be provided in the PSP submittal according to § 236.907 (a) (7), and to eliminate an alternative option for a railroad to use a risk metric in which consequences of potential accidents are measured strictly in terms of fatalities.

Currently paragraph § 236.909 (e) (1), while discussing how safety and risk are measured for the full risk assessment, does not accentuate the need for running a sensitivity analysis on chosen risk metrics to assure that the worst case scenarios for the proposed system failures or malfunctions are accounted for in the risk assessment. On the other hand, the Appendix B to this part mandates that each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis. The FRA's experience gained while reviewing first PSP documents required by Subpart H and submitted to FRA for approval, showed that it did not appear mandatory for the railroads to run a sensitivity analysis for the chosen risk metrics. An additional effort was required from the FRA officials reviewing PSP submittals to demonstrate to the railroads the validity and significance of such a request. Therefore, FRA considers it necessary to include the requirement for a sensitivity analysis to be run for the chosen risk metrics in the final rule itself. The modified text of this paragraph explains why the sensitivity analysis is needed and what key input parameters must be analyzed.

A sensitivity analysis must be conducted by defining the range of values (i.e. lower bound, upper bound, and associated distribution) for key input parameters and assessing the impact of variations over those ranges on the overall system risk. The worst case analysis must consider realistic combinations of these key parameters as they tend toward their worst case values. Justification must be provided for the ranges and process used in the design of the sensitivity analysis.

Paragraph § 236.909 (e) (2) is modified to clarify how the exposure and consequences, as main components of risk computation formula, must be measured. It is outlined that the exposure must be measured in train-miles per year over the relevant railroad infrastructure where a proposed system is to be implemented. The consequences of potential accidents must identify the total cost, including fatalities, injuries, property damage and other incidental costs. The alternative risk metric, previously allowing to measure consequences strictly in terms of fatalities is eliminated from this paragraph. The first years of the Final Rule implementation revealed that measuring consequences of accidents strictly in term of fatalities did not serve as an adequate alternative to metrics of total cost of accidents for two main reasons. First of all, the statistical data on railroad accidents shows that accidents involving fatalities also cause injuries and significant damage to railroad property and infrastructure for both freight and especially passenger operations. Even though the cost of human life is always the highest component of monitory estimates of accident consequences, the dollar estimates of injuries, property losses, and damage to the environment associated with accidents involving fatalities cannot and should not be discounted in the risk analysis. Secondly, allowing fatalities to serve as the only risk metrics of accidents consequences happened to be confusing to the industry and got misinterpreted by the risk assessment analysts attempting to determine the overall risk associated with the use of certain type of train control system. This provoked some risk analysts to inappropriately convert injuries and property damages for observed accidents into relative estimates of fatalities. This method cannot be considered acceptable because while distorting the overall picture of accident consequences it also raises questions on appropriateness of conversion coefficients. Therefore, FRA considers appropriate to eliminate from the rule the alternative option for consequences to be measured in fatalities only.

FRA Re-Draft After Comments,
September 2, 2009

**PTCWG09-08-31,01,02-04 WG CONSENSUS FINAL 236.909 CLEAN consolidated document**

**Proposed Changes to Risk-related Sections of NPRM**

**1. Preamble**

* * *

**§ 236.909 Minimum Performance Standard**

Formatted: Line spacing: single

FRA is modifying existing § 236.909 to include a requirement for the risk metric sensitivity analysis to be an inherent part of the full risk assessment that is to be provided in the PSP submittal according to § 236.907 (a) (7), and to eliminate an alternative option for a railroad to use a risk metric in which consequences of potential accidents are measured strictly in terms of fatalities.

Currently paragraph § 236.909 (e) (1), while discussing how safety and risk are measured for the full risk assessment, does not accentuate the need for running a sensitivity analysis on chosen risk metrics to assure that the worst case scenarios for the proposed system failures or malfunctions are accounted for in the risk assessment. On the other hand, the Appendix B to this part mandates that each risk metric for the proposed product must be expressed with an upper bound, as estimated with a sensitivity analysis. The FRA's experience gained while reviewing first PSP documents required by Subpart H and submitted to FRA for approval, showed that it did not appear mandatory for the railroads to run a sensitivity analysis for the chosen risk metrics. An additional effort was required from the FRA officials reviewing PSP submittals to demonstrate to the railroads the validity and significance of such a request. Therefore, FRA considers it necessary to include the requirement for a sensitivity analysis to be run for the chosen risk metrics in the final rule itself. The modified text of this paragraph explains why the sensitivity analysis is needed and what key input parameters must be analyzed.

A sensitivity analysis must be conducted by defining the range of values (i.e. lower bound, upper bound, and associated distribution) for key input parameters and assessing the impact of variations over those ranges on the overall system risk. The worst case analysis must consider realistic combinations of these key parameters as they tend toward their worst case values. Justification must be provided for the ranges and process used in the design of the sensitivity analysis.

Paragraph § 236.909 (e) (2) is modified to clarify how the exposure and consequences, as main components of risk computation formula, must be measured. It is outlined that the exposure must be measured in train-miles per year over the relevant railroad infrastructure where a proposed system is to be implemented. The consequences of potential accidents must identify the total cost, including fatalities, injuries, property

damage and other incidental costs. The alternative risk metric, previously allowing to measure consequences strictly in terms of fatalities is eliminated from this paragraph. The first years of the Final Rule implementation revealed that measuring consequences of accidents strictly in term of fatalities did not serve as an adequate alternative to metrics of total cost of accidents for two main reasons. First of all, the statistical data on railroad accidents shows that accidents involving fatalities also cause injuries and significant damage to railroad property and infrastructure for both freight and especially passenger operations. Even though the cost of human life is always the highest component of monitory estimates of accident consequences, the dollar estimates of injuries, property losses, and damage to the environment associated with accidents involving fatalities cannot and should not be discounted in the risk analysis. Secondly, allowing fatalities to serve as the only risk metrics of accidents consequences happened to be confusing to the industry and got misinterpreted by the risk assessment analysts attempting to determine the overall risk associated with the use of certain type of train control system. This provoked some risk analysts to inappropriately convert injuries and property damages for observed accidents into relative estimates of fatalities. This method cannot be considered acceptable because while distorting the overall picture of accident consequences it also raises questions on appropriateness of conversion coefficients. Therefore, FRA considers appropriate to eliminate from the rule the alternative option for consequences to be measured in fatalities only.

* * *

**2. The Rule**

* * *

9. Section 236.909 is amended by adding a new sentence directly after the first sentence of paragraph (e)(1) and by revising paragraph (e)(2)(i) to read as follows:

Formatted: Line spacing: single

§ 236.909 Minimum performance standards.

* * * * *

(e) * * *

(1) * * * The total risk assessment must have a supporting sensitivity analysis. The analysis must confirm that the risk metrics of the system are not negatively affected by sensitivity analysis input parameters including, for example, component failure rates, human factor error rates, and variations in train traffic affecting exposure. In this context, "negatively affected" means that the final residual risk metric does not exceed that of the base case or otherwise established through MTTHE target. The sensitivity analysis must document the sensitivity to worst case failure scenarios.

Formatted: Font: Not Bold

* * *

(2) * * *

(i) In all cases exposure must be expressed as total train miles traveled per year over the relevant railroad infrastructure. Consequences must identify the total cost, including fatalities, injuries, property damage, and other incidental costs, such as

potential consequences of hazardous materials involvement, resulting from preventable accidents associated with the function(s) performed by the system.

* * * * *

11. Revise Appendix B to part 236 to read as follows:

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 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. ~~Such failure frequency~~ 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 ~~proper~~ 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.

**Formatted:** Font: Not Bold

**Formatted:** Font color: Auto

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold

**Formatted:** Font: Not Bold

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 ~~automated~~ 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 which permits the railroad to project the likelihood of detecting an in-service software defect. These assumptions shall be documented in such a form as to permit later ~~automated~~ comparisons with in-service experience.

(4) The railroad shall document all of the identified safety-critical fault paths 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.

12. Revise Appendix C to read as follows:

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. Absence of specific operator actions or procedures will not prevent the system from operating safely. The designer must identify and categorize all hazards that may lead to unsafe system operation. Hazards categorized as unacceptable ~~or undesirable~~, which is determined by hazard analysis, must be eliminated by design. Best effort shall be made by the designer to also 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 or eliminate unsafe systematic failures--those conditions which can be attributed to human error that could occur at various stages throughout product development. This includes unsafe errors in the software due to human error in the software specification, design or coding phases, or both; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

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

**Formatted:** Font: Not Bold

(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 ~~before falsely activating~~ 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 ~~before falsely activating~~ that eliminates the possibility of false activation of any physical appliance.

**Deleted:** ¶

(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-Part3: Software requirements.

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

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

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

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

(H) IEC62278: 2002, Railway Applications: Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS);

(I) IEC62279: 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.