DEPARTMENT OF TRANSPORTATION

Federal Railroad Administration

49 CFR Parts 209, 234, and 236

[Docket No. FRA–2001–10160]

RIN 2130–AA94

Standards for Development and Use of Processor-Based Signal and Train Control Systems

AGENCY: Federal Railroad Administration (FRA), Department of Transportation (DOT).

ACTION: Final rule.

SUMMARY: FRA is issuing a performance standard for the development and use of processor-based signal and train control systems. The rule also covers systems which interact with highway-rail grade-crossing warning systems. The rule establishes requirements for notifying FRA prior to installation and for training and recordkeeping. FRA is issuing these standards to promote the safe operation of trains on railroads using processor-based signal and train control equipment.

DATES: This rule is effective June 6, 2005. The incorporation by reference of a certain publication listed in the rule is approved by the Director of the Federal Register as of June 6, 2005.

ADDRESSES: Except for good cause shown, any petition for reconsideration of any part of this rule must be submitted not later than May 6, 2005. Any petition for reconsideration should reference FRA Docket No. FRA–2001–10160 and be submitted in triplicate to the Docket Clerk, Office of Chief Counsel, FRA, 1120 Vermont Avenue, NW., Mail Stop 10, Washington, DC 20590. Petitions, received by the FRA Docket Clerk will be sent to the DOT Docket Management System (DMS) located on the Plaza level of the Nassif Building at the Department of Transportation. You can review public dockets, including any petitions for reconsideration received there between the hours of 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You can also review any petition for reconsideration on-line at the DMS Web site at *http://dms.dot.gov.* Please note that anyone is able to search the electronic form of all submissions into any of FRA's dockets by the name of the individual making the submission (or signing the submission, if submitted on behalf of an association, business, labor union, etc.). You may review DOT's complete Privacy Act Statement in the **Federal Register** published on April 11, 2000 (volume 65, number 70; pages 19477–78), or you may visit *http://dms.dot.gov.*

FOR FURTHER INFORMATION CONTACT: Tom McFarlin, Staff Director, Signal and Train Control Division, Office of Safety, FRA, 1120 Vermont Avenue, NW., Mail Stop 25, Washington, DC 20590 (telephone: 202–493–6203); or Melissa Porter, Office of Chief Counsel, FRA, 1120 Vermont Avenue, NW., Mail Stop 10, Washington, DC 20590 (telephone: 202–493–6034).

SUPPLEMENTARY INFORMATION:

Table of Contents for Supplementary Information

I. Introduction

FRA is issuing a performance standard for processor-based signal and train control systems. FRA began the process of developing a rule in 1997 when its Railroad Safety Advisory Committee (RSAC) was tasked with developing a proposed rule for FRA's consideration. RSAC made consensus recommendations to FRA on a proposed rule; FRA agreed to these recommendations and published them as a notice of proposed rulemaking (NPRM) on August 10, 2001 (66 FR 42352). FRA received quite a few public comments on the NPRM. This notice responds to comments on the NPRM and issues the final rule. The standards grew out of the proposed rule requiring that processor-based signal and train control systems meet or exceed the safety level of the traditional signal systems they replace. The preamble discusses the statutory background, the regulatory background, the RSAC proceedings, the alternatives considered and the rationale for the option selected, the proceedings to date, as well as the comments and conclusions on general issues. Other comments and resolutions are discussed within the corresponding section-by-section analysis.

II. Statutory Background

FRA has broad statutory authority to regulate all areas of railroad safety. 49 U.S.C. 20103(a); 49 CFR 1.49. The Federal Railroad Safety Act of 1970, Public Law 91–458, contained this broad grant of authority and supplemented the older rail safety laws then in existence. The older safety laws had been enacted in a piecemeal approach and addressed specific fields of railroad safety. For instance, the Signal Inspection Act, 49 U.S.C. 26 (recodified at 49 U.S.C. 20502 *et seq.* (1994)), has governed the installation and removal of signal equipment since its enactment August 26, 1937. Until July 5, 1994, the Federal railroad safety statutes existed as separate acts found primarily in Title 45 of the United States Code. On that date all of the acts were repealed and their provisions were recodified into Title 49 Chapters 201–213.

Pursuant to its general statutory rulemaking authority, FRA promulgates and enforces rules as part of a comprehensive regulatory program to address the safety of railroad track, signal systems, railroad communications, rolling stock, operating practices, passenger train emergency preparedness, alcohol and drug testing, locomotive engineer certification, and workplace safety. In the area of railroad signal and train control systems, FRA has issued regulations, found at 49 CFR part 236 (''part 236''), addressing topics such as the security of signal apparatus housings against unauthorized entry (49 CFR 236.3), location of roadway signals (49 CFR 236.21), and the testing of relays (49 CFR 236.106). Hereafter all references to parts and sections shall be parts and sections located in Title 49 of the Code of Federal Regulations.

FRA continually reviews its regulations and revises them as needed to keep up with emerging technology. FRA's need to review its regulatory

scheme with respect to emerging technology in the signal and train control arena was acknowledged by Congress in Section 11 of the Rail Safety Enforcement and Review Act (RSERA) (Pub. L. 102–365, Sep. 3, 1992), entitled ''Railroad Radio Communications.'' Section 11(a) of RSERA mandated that the Secretary conduct a safety inquiry to assess, among other areas,

(6) The status of advanced train control systems that are being developed, and the implications of such systems for effective railroad communications; and

(7) The need for minimum Federal standards to ensure that such systems provide for positive train separation and are compatible nationwide.

106 Stat. 980. Section 11(b) required the Secretary to

submit to Congress within 4 months after the completion of such inquiry a report on the results of the inquiry along with an identification of appropriate regulatory action and specific plans for taking such action.

Id.

FRA conducted the inquiry required by RSERA and submitted a comprehensive Report to Congress on July 8, 1994, entitled *Railroad Communications and Train Control* (1994 PTC Report). A copy of this 1994 PTC Report is in the docket of this rulemaking. As part of the 1994 PTC Report, FRA called for implementation of an action plan to deploy PTC systems. The report forecast substantial benefits of advanced train control technology to support a variety of business and safety purposes, but noted that an immediate regulatory mandate for PTC could not be currently justified based upon normal cost/benefit principles relying on direct safety benefits. The report outlined an aggressive Action Plan implementing a public/private sector partnership to explore technology potential, deploy systems for demonstration, and structure a regulatory framework to support emerging PTC initiatives.

Since 1994, the Congress has appropriated and FRA has committed approximately $40 million through the Next Generation High Speed Rail Program and the Research and Development Program to support development, testing and deployment of PTC prototype systems in Illinois, Alaska, and the Eastern railroads' on-board electronic platforms. As called for in the Action Plan, the FRA also launched an effort to structure an appropriate regulatory framework for facilitating implementation of PTC technology and for evaluating future safety needs and opportunities. For such a task, FRA desired input from the developers, prospective purchasers and operators of this new technology. Thus, in September of 1997, the Federal Railroad Administrator asked RSAC to address several issues involving PTC, including the development of performance standards for PTC systems. RSAC's involvement in this rulemaking will be discussed later in the preamble.

Since the issuance of FRA's 1994 PTC Report, Congress has twice requested the Secretary of Transportation to submit additional reports on PTC; first in 1994, and more recently in 2003. In 1994, Congress directed the Secretary to submit a progress report.

The Secretary of Transportation shall submit a report to the Congress on the development, deployment, and demonstration of positive train control systems by December 31, 1995.

49 U.S.C. 20150. On May 17, 2000, FRA submitted a letter report responding to Section 20150 (2000 PTC Report). A copy of the 2000 PTC Report is in the docket of this rulemaking. The report noted the progress being made toward the deployment of PTC systems but concluded that deployment on the entire national rail system cannot be justified on safety grounds alone. FRA indicated that it would continue to encourage railroads to deploy PTC voluntarily. The report noted that RSAC, at FRA's request, had begun to address the PTC issue, and had issued a report to FRA in September 1999 (1999 RSAC Report) entitled *Implementation of Positive Train Control Systems* that detailed current PTC system projects, estimated accidents preventable by PTC systems, and estimated the costs and benefits of PTC systems as applied to the major railroads.

The 1999 RSAC Report confirmed the core PTC safety functions described in the 1994 PTC Report (prevent train-to-train collisions; enforce speed restrictions and temporary slow orders; and provide protection for roadway workers and their equipment operating under specific authorities). It also referred to additional safety functions that might be included in some PTC architecture (*e.g.*, warning of on-track equipment operating outside the limits of authority; enforcement of hazard detection warnings; and a future capability for generating data for transfer to highway users to enhance warning at highway-rail grade crossings).

The 1999 RSAC Report found that railroad safety benefits of PTC could not support the investments necessary to deploy the system. The report estimated that PTC deployment on the Class 1 railroads would cost about $1.2 billion to equip the lines with a level 1 type PTC system (address core PTC functions only), and about $7.8 billion to equip the lines with a level 4 type PTC system (increased functionality addressing additional safety monitoring systems and enhanced traffic management capabilities). These costs are total discounted life cycle costs, including procurement, installation, and maintenance, over 20 years. The 20 year total discounted benefits from avoided accidents ranged from about $500 million for a level 1 PTC system, to about $850 million for a level 4 PTC system. The Committee was not able to reach conclusions regarding the non-safety benefits of PTC-related technologies.

As part of the FRA appropriations for fiscal year 2003, Congress requested FRA to update cost/benefit numbers contained in the 2000 PTC Report to Congress. The Conference Report on the Consolidated Appropriations Resolution, 2003 (Pub. L. 108–7) provided in pertinent part as follows:

Positive train control.—The conferees direct FRA to submit an updated economic analysis of the costs and benefits of positive train control and related systems that takes into account advances in technology and system savings to carriers and shippers as well as other cost savings related to prioritized deployment of these systems, as proposed by the Senate. This analysis must be submitted as a letter report to the House and Senate Committees on Appropriations by October 1, 2003.

H.R. Rep. No. 108–10, 108th Cong. 1st Sess. 1286–7. FRA submitted the requested PTC letter report to Congress on August 18, 2004 and a copy of the report is in the docket of this rulemaking. The report indicates that substantial public benefits would likely flow from the installation of PTC systems on the railroad system, although the total amount of these benefits is subject to debate. The report reaffirmed the conclusions reached in the 1994 and 2000 PTC Reports that the safety benefits of PTC systems are relatively small in comparison to the huge costs of installing the PTC systems.

In light of the cost/benefit numbers, an immediate regulatory mandate for PTC could not be currently justified based upon normal cost/benefit principles relying on direct railroad safety benefits. FRA has, therefore, chosen to issue a final rule that establishes a performance standard for processor-based train control systems, but does not require that they be installed. PTC systems can enhance the

safety of railroad operations; the rule will help facilitate the establishment of such systems.

III. Regulatory Background

Part 236 was last amended in 1984. At that time, signal and train control functions were performed principally through use of electrical circuits employing relays as the means of effecting system logic. This approach had proven itself capable of supporting a very high level of safety for over half a century. However, electronic controls were emerging on the scene, and several sections of the regulations were amended to take a more technology-neutral approach to the required functions (*see* §§ 236.8, 236.51, 236.101, 236.205, 236.311, 236.813a). This approach has fostered introduction of new, more cost effective technology while providing FRA with strong enforcement powers over systems that fail to work as intended in the field.

Since that time, FRA has worked with railroads and suppliers to apply the principles embodied in the regulations to emerging technology and to identify and remedy initial weaknesses in some of the new products. As a result, thousands of interlocking controllers and other electronic applications are embedded in traditional signal systems. Further technological advances may provide additional opportunities to increase safety levels and achieve economic benefits as well. For instance, implementation of innovative PTC systems may employ new ways of detecting trains, establishing secure routes, and processing information. This presents a far greater challenge to both signal and train control system developers and FRA. This challenge involves retaining a corporate memory of the intricate logic associated with railway signaling, while daring to use whole new approaches to implement that logic—at the same time stretching the technology to address risk reduction opportunities that previously were not available. For FRA, the challenge is to continue to be prepared to make safety-based decisions regarding this new technology, without impairing the development of this field. Providing general standards for the development and implementation of products utilizing this new technology is necessary to facilitate realization of the potential of electronic control systems and for safety and efficiency.

FRA has already used its safety authority to grant waivers and issue orders to support innovation in the field of train control technology. FRA has granted test waivers for the Union Pacific Railroad Company (UP)/Burlington Northern and Santa Fe Railway Company (BNSF) Positive Train Separation (PTS) project in the Pacific Northwest, the National Railroad Passenger Corporation (Amtrak) Incremental Train Control System (ITCS) in the State of Michigan, the CSX Transportation, Inc. (CSXT) Communication-Based Train Management (CBTM) project in South Carolina and Georgia, and the Alaska Railroad PTC project. On September 19, 1996 FRA granted conditional revenue demonstration authority for ITCS. In 1998, FRA issued a final order for the installation of the Advanced Civil Speed Enforcement System (ACSES) on the Northeast Corridor (63 FR 39343, Aug. 21, 1998). See also 64 FR 54410, Oct. 6, 1999 (delaying effective date of such order).

Although FRA expects to continue its support for these current projects, the need for controlling principles in this area has become patently obvious. This rulemaking has provided a forum for identifying and codifying those principles.

IV. RSAC

A. Overview

In March 1996, FRA established the RSAC, which provides a forum for consensual rulemaking and program development. The Committee includes representation from all of the agency's major customer groups, including railroads, labor organizations, suppliers and manufacturers, and other interested parties. A list of member groups follows:

American Association of Private Railroad Car Owners (AARPCO)
American Association of State Highway & Transportation Officials (AASHTO)
American Public Transportation Association (APTA)
American Short Line and Regional Railroad Association (ASLRRA)
American Train Dispatchers Department/ Brotherhood of Locomotive Engineers (ATDD/BLE)
Amtrak
Association of American Railroads (AAR)
Association of Railway Museums (ARM)
Association of State Rail Safety Managers (ASRSM)
Brotherhood of Locomotive Engineers (BLE)
Brotherhood of Maintenance of Way Employees (BMWE)
Brotherhood of Railroad Signalmen (BRS)
Federal Transit Administration (FTA)*
High Speed Ground Transportation Association
Hotel Employees & Restaurant Employees International Union
International Association of Machinists and Aerospace Workers
International Brotherhood of Boilermakers and Blacksmiths
International Brotherhood of Electrical Workers (IBEW)
Labor Council for Latin American Advancement (LCLAA)*
League of Railway Industry Women*
National Association of Railroad Passengers (NARP)
National Association of Railway Business Women*
National Conference of Firemen & Oilers
National Railroad Construction and Maintenance Association
National Transportation Safety Board (NTSB)*
Railway Progress Institute (RPI)
Safe Travel America
Secretaria de Communicaciones y Transporte*
Sheet Metal Workers International Association
Tourist Railway Association Inc.
Transport Canada*
Transport Workers Union of America (TWUA)
Transportation Communications International Union/BRC (TCIU/BRC)
United Transportation Union (UTU)

*Indicates associate membership.

When appropriate, FRA assigns a task to RSAC, and after consideration and debate, RSAC may accept or reject the task. If accepted, RSAC establishes a working group that possesses the appropriate expertise and representation of interests to develop recommendation] to FRA for action on the task. These recommendations are developed by consensus. The working group may establish one or more task forces or other subgroups to develop facts and options on a particular aspect of a given task. The task force or other subgroup reports for the working group. If a working group comes to consensus on recommendations for action, the package is presented to the RSAC for a vote. If the proposal is accepted by a simple majority of the RSAC, the proposal is formally recommended to FRA. FRA then determines what action to take on the recommendation. Because FRA staff has played an active role at the working group and subgroup levels in discussing the issues and options and in drafting the language of the consensus proposal and because the RSAC recommendation constitutes the consensus of some of the industry's leading experts on a given subject, FRA is often favorably inclined toward the RSAC recommendation. However, FRA is in no way bound to follow the recommendation and the agency exercises its independent judgement on whether the recommended rule achieves the agency's regulatory goal, is soundly supported, and is in accordance with policy and legal requirements. Often, FRA varies in some respects from the RSAC recommendation in developing the actual regulatory proposal. If the working group is unable to reach consensus on recommendations for

action, FRA moves ahead to resolve the issue through traditional rulemaking proceedings.

B. The PTC Working Group

On September 30, 1997, the RSAC accepted a task (No. 97–6) entitled ''Standards for New Train Control Systems.'' The purpose of this task was defined as follows: ''To facilitate the implementation of software based signal and operating systems by discussing potential revisions to the Rules, Standards and Instructions (Part 236) to address processor-based technology and communication-based operating architectures.'' The task called for the formation of a working group to include consideration of the following:

- Disarrangement of microprocessor-based interlockings;
- Performance standards for PTC systems at various levels of functionalities (safety-related capabilities); and
- Procedures for introduction and validation of new systems.

RSAC also accepted two other tasks related to PTC, task Nos. 97–4 and 97–5. These tasks dealt primarily with issues related to the feasibility of implementation of PTC technology.

FRA gratefully acknowledges the participation and leadership of representatives of the following organizations who served on the PTC Working Group (hereafter Working Group):

AAR, including members from
  BNSF
  Canadian National
  Consolidated Rail Corporation
  CSX
  Metra
  Norfolk Southern Railway Company
  UP
AASHTO
Amtrak
APTA
ASLRRA
ATDD/BLE
BLE
BMWE
BRS
FRA
High Speed Ground Transportation Association
IBEW
RPI
UTU

Staff from the National Transportation Safety Board and the Federal Transit Administration also participated in an advisory capacity.

In order to efficiently accomplish the three tasks assigned to it involving PTC issues, the Working Group empowered two task forces to work concurrently: The Data and Implementation Task Force, which handled tasks 97–4 and 97–5, and the Standards Task Force, which handled task 97–6.

The Data and Implementation Task Force finalized a report on the future of PTC systems and presented it, with the approval of RSAC, to the Administrator in September of 1999. Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator, ''Implementation of Positive Train Control Systems'' (September 8, 1999).

The Working Group also employed several teams, comprised of representatives from RSAC member organizations, who provided invaluable assistance. An Operating Rules Team was charged with working to ensure that appropriate railroad operating rules are part of any PTC implementation process, and a Human Factors Team was charged with evaluating human factor aspects of PTC systems. Members of these teams serve on both the PTC Standards Task Force and the Data and Implementation Task Force, and additional team members were drawn from the railroad community.

FRA staff and staff from the Volpe National Transportation Systems Center (the Volpe Center) worked with the Working Group and its subgroups. FRA responded to a consensus request from the Standards Task Force by contracting for assistance from the Center for Safety-Critical Systems at the University of Virginia.

The NPRM describes the role the Standards Task Force played in developing its recommendations to the Working Group and RSAC, which were in turn recommended to FRA by RSAC and formed the basis for the proposed rule. The Standards Task Force ceased to meet and exist after publication of the NPRM. References to the Standards Task Force and Working Group are reiterated here to provide a historical perspective regarding development of the RSAC recommendations on which the NPRM was based. These points are discussed to show the origin of certain issues and the course of discussion on these issues at the Task Force and Working Group levels. We believe this helps illuminate the factors FRA weighed in making its regulatory decisions at the NPRM stage, and the logic behind those decisions, most of which are still embodied in this final rule.

V. Discussion of Alternatives Considered and the Rationale for the Option Selected

As previously noted, RSAC recommended to FRA that it adopt the proposed rule recommended to RSAC by the Working Group. FRA concluded that the recommended proposed rule would satisfy its regulatory goals and issued an NPRM that tracked the RSAC recommendation on all major issues. Subsequent to the publication of the NPRM and the close of the comment period, informative discussions were had at the RSAC Working Group meetings regarding issues and concerns raised by written comments. These discussions contributed greatly to FRA's knowledge and understanding of the relevant subject matter, but, as discussed below, RSAC was ultimately unable to reach consensus on recommendations regarding the final rule.

In this final rule, FRA has carried forward the basic principles and structure and in many cases the language of the proposed rule with few or no changes, as initially recommended by the RSAC at the NPRM stage. The text of the final rule is substantially different from the NPRM in only a few ways. First, FRA is adding a provision delineating the responsibilities of railroads and suppliers regarding software hazards; second, FRA is providing alternatives for the abbreviated risk assessment; third, FRA is providing criteria for adjustment to the base case where changes are planned in the subject operation's speed and density; fourth, FRA is adding a provision as notice that entities may be subject to criminal penalties in accordance with 49 U.S.C. 21311; and last, FRA is adding an appendix with a schedule of civil penalties. In addition, minor edits for improved clarity and consistency have been added. Each of these substantive changes will be addressed in the section-by-section analysis of the rule text to which it applies. However, given the failure of RSAC to reach consensus at the final rule stage, FRA has determined the contents of the final rule, without the benefit of a formal RSAC recommendation, based on the agency's best judgment (informed, in many cases, by the excellent discussion of the issues within the Working Group).

A. Performance Standards vs. Prescriptive Standards

During early discussions in the advisory process, FRA noted that the existing ''Rules, Standards and Instructions'' (part 236) take a performance-oriented approach at the functional level, although—by virtue of the historical context in which they were initially prepared—they most often reference older technology. During the last decade and a half, this performance-oriented approach to specified functions has permitted the growth of electronic systems within signal and train control

systems without substantial regulatory change (albeit with growing ambiguity concerning the application of individual provisions to novel technical approaches). Wishing to maintain historical continuity and hasten preparation of a proposed and ultimately a final rule, FRA offered for consideration an initial redraft of part 236 that attempted a more technology-neutral approach to performance at the functional level, while also addressing PTC functions, as a possible starting point for the group's work.

Carrier representatives found the FRA draft to be unduly constricting, and asked thatthe group pursue higher-level performance standards. Supplier and labor representatives agreed to this approach, and FRA endeavored to support the Standards Task Force in pursuing it.

The group heard from representatives of the Research and Special Programs Administration, Federal Highway Administration's Office of Motor Carrier Safety (now Federal Motor Carrier Safety Administration), and APTA. FRA distributed a guidance document entitled ''Performance Standards: A Practical Guide to the Use of Performance Standards as a Regulatory Alternative,'' (Project on Alternative Regulatory Approaches, September 1981), a copy of which has been placed in the docket of this rulemaking.

In brief overview, the term ''performance standard'' has been variously applied to describe many different forms of regulatory approaches that avoid design specifications and other prescriptive requirements, such as mandates that actions be taken in a particular sequence, or in a particular manner, by the regulated entity. At the most permissive extreme, a performance standard for a railroad operating system might specify an ''acceptable'' level of safety performance (*e.g.*, number of fatalities per million train miles) and avoid any intervening action unless and until the performance of the regulated entity fell below that level. FRA believes that this type of approach would represent an abandonment of the agency's responsibility to promote safety, since it would necessarily assume optimum performance by the regulated entity (a condition not realized in practice) and would prevent helpful intervention until unacceptable consequences had already occurred. FRA has not sought to pursue this approach.

The least permissive performance standards include such approaches as requiring that a metal skin on the front of a locomotive have penetration resistance equivalent to that of a given thickness of a specified steel. In this example, the choice of material is left to the designer, but the options are not extensive. See, *e.g.*, § 238.209.

In the middle range of permissiveness, a performance standard might address acceptable performance parameters for a particular, mandated device, in lieu of a fixed physical description. For instance, FRA requirements for railroad tank cars carrying flammable compressed gas require the application of high temperature thermal protection that can be accomplished using a variety of materials, together with pressure relief valve capacity requirements adequate to permit safe evacuation and burn-off of the car's contents prior to catastrophic failure of the vessel in a fire environment (part 179, Appendix B (qualification test procedure)). This combination of regulatory requirements has been highly effective in preventing loss of life from violent detonation of tank cars involved in derailments (although compliance issues have been presented by disintegration of insulation blankets that could not be readily detected under the outer jacket of a car).

Some of the safety statutes administered by FRA contain performance-based criteria. For instance, the Signal Inspection Act, as codified at 49 U.S.C. 20502(b), states:

> A railroad carrier may allow a signal system to be used on its railroad line only when the system, including its controlling and operating appurtenances * * * may be operated safely without unnecessary risk of personal injury.

However, recognizing the need to make a practical application of this broad statement, the law also requires that the system ''has been inspected and can meet any test prescribed under this chapter.'' What could otherwise be deemed a very broad performance standard is thus made more specific in practice.

B. Evaluation of Perfomance-Based Approach

The NPRM identified a variety of considerations relevant to whether, and in what form, performance standards should be employed in this and other settings. After review of the public comments on the NPRM, FRA is satisfied that, as a general matter, the performance standard contained in the final rule should be suitable for this context. That is—

- The standard is stated as a practical goal;
- It will be enforceable;
- It will be usable by small entities;
- It can be shown to yield safety that is equivalent to that required under the existing Rules, Standards and Instructions (RS&I) issued by FRA's predecessor the Interstate Commerce Commission (ICC) and carried forward by FRA in part 236;
- Its cost is reasonable;
- It provides means of determining compliance before safety is endangered; and
- As adapted in this final rule, analytical techniques needed to verify compliance are available.

This last point bears further mention. FRA expressed concern in the NPRM that a risk assessment technique, the Axiomatic Safety-Critical Assurance Process(ASACP), intended to provide an important toolset to establish compliance with the performance standard was still under development. Although that continued to be the case as FRA was preparing this final rule and submitting it for review and clearance, FRA has made appropriate changes to this final rule emphasizing FRA's conclusion that more than one type of risk assessment is acceptable.

FRA had also identified several desirable criteria with respect to promulgating a performance standard specifically for processor-based signal and train control technologies: Simplicity, relevancy, reliability, cost, and objectivity.

Simplicity: Although nothing about producing a safety-critical signal or train control system is inherently simple, the final rule is relatively simple and provides the railroads with a great deal of flexibility.

Relevancy: Like the NPRM, the final rule focuses on the safety-relevant characteristics of systems and emphasizes all relevant aspects of product performance.

Reliability: This criterion could also be referred to as precision. That is, the standard should be reliable in that the test applied should yield similar results each time it is applied to the same subject matters. This criterion remains a concern in relation to the functioning of the final rule, but FRA has determined that the challenges presented should be manageable.

Cost: FRA pointed out in the NPRM that demonstrating compliance with the standard should not be unduly expensive. In reviewing the comments and making adjustments to the final rule, FRA has structured a standard that is not unduly expensive.

Objectivity: A completely objective standard would allow for compliance to be determined through scientific study or investigation. This is another dimension of enforceability. Like the NPRM, the final rule includes a number of provisions intended to ensure that

application of the standard will be demonstrably objective.

C. Advantages of a Performance-Based Standard; Consideration of Disadvantages

This final rule presents the highest level performance requirements ever attempted by FRA. In the NPRM, FRA discussed at length both the reasons to pursue such a course and concerns perceived by the agency regarding its wisdom.

Since issuance of the NPRM, FRA has continued its inquiries into the advantages and limitations of high-level performance standards and the current utility of available risk assessment techniques to determine compliance with such standards. See, *e.g.,* Coglianese, Nash, and Olmstead, Performance-Based Regulation: Prospects and Limitations in Health, Safety, and Environmental Protection (Regulation Policy Program, John F. Kennedy School of Government, Harvard University 2002). FRA has been impressed both by the potential power of performance standards to foster innovation and by the fact that most regulatory implementations of the concept have been layered on top of prescriptive standards rather than replacing them. That is, practice in most agencies with similar missions has focused on being ''risk informed'' rather than ''risk driven.'' The fundamental reason for this is the inherent difficulty of predicting safety outcomes in complex environments.

FRA remains concerned that the performance-based approach of this final rule may not ensure progressive improvements in safety. Risk management practitioners typically set goals for incremental improvements in safety in connection with use of performance standards. By contrast, this final rule makes current risk levels the floor for future performance. However, if reductions in risk levels do not occur as part of the natural progression from application of the rule's performance based standards, the improvement in risk levels can be achieved by regulatory mandate. FRA refers in the final rule to the prerogative of the agency to order improvements in safety where they are supported by appropriate analysis.

In the NPRM, FRA also expressed doubt regarding whether the relevant technical, scientific, and railroad signaling communities are fully prepared to support implementation of the proposed rule. Although commenters did not appear to question the fact that the field of safety-critical systems is relatively new and undergoing a process of maturation, they did question some of FRA's assertions. For instance, a major signal supplier noted that suppliers do provide quantitative information concerning life-cycle safety performance in the transit market. The same supplier stated that the concept of product validation is much better settled than suggested by FRA in the NPRM and questioned FRA's suggestion that quantifying risk with respect to electronic systems was somehow more difficult than with electro-mechanical systems. Notably, however, the supplier was addressing this topic from the context of design and production of systems utilizing traditional safety concepts. The same commenter noted that much more challenging issues associated with less conventional systems (including those relying upon complex commercial off-the-shelf hardware or software for which source code is not available to the designer and where changes may be introduced without notice).

Commenters generally did not question the difficulty associated with assigning values to human factor risk, and FRA's consideration of the issues as informed by intervening discussions of the Working Group (including presentation and discussion of various risk assessment topics) has done nothing to call into question FRA's original concerns regarding the complexity of safety proofs at the system level, particularly where human factors or non-conventional electronic systems are involved.

Neither did commenters effectively reassure FRA regarding the danger that risk assessment could become an ''after the fact'' justification for a system already constructed. This concern could be exacerbated by the difficulty of conducting risk assessments in parallel with product development against tight time deadlines. Under such circumstances, the tendency is to assign each subsystem of the electronic system a ''risk budget,'' after which the temptation to stay within budget could have the tendency to skew estimates. FRA has removed a sentence from the appendix on risk assessment that could be read to endorse this approach; but there is, of course, no reasonable way to prevent it from occurring. Rather, FRA will need to be alert to this procedure; and, where it is used, it may be appropriate to require a third party assessment of the verification and validation process that yielded the compliant estimates.

D. Analysis of Risk Associated With Train Control Technologies

As reported in the NPRM, recognizing the need to advance the state of the art with respect to analysis of risk specifically associated with various methods of operations and train control technologies, the Standards Task Force established a team to support development of a ASCAP. At the request of the Standards Task Force, FRA engaged the University of Virginia (UVA) to develop the ASCAP model as a risk assessment ''toolkit'' for use in implementing the PTC rule then under development. The initial challenge for the ASCAP team and contractor was to describe the level of risk associated with the current method of operation on a CSXT line, which is operated without a signal system using direct traffic control system rules (the ''base case''). The first comparison case was to be the operations on the same line should a traffic control system be installed. The second comparison case was to be implementation of the proposed Communications Based Train Management (CBTM) system, an innovative technology that addresses the PTC core functions.

As the effort progressed, the traffic control case was eliminated and the effort focused on CBTM. This ''dry run'' for ASCAP resulted in development of important elements of the technique, including a relatively sophisticated train management algorithm. The CBTM exercise was then suspended due to the need for the University to focus on the safety case for the Illinois DOT Project under contract to System Designer and Integrator for the North American Joint Positive Train Control Program (NAJPTC). When UVA last briefed the RSAC Working Group on this effort in March of 2003, it was clear that the method had been greatly enriched; however, neither the adjusted base case nor the PTC case had yet been finalized. Due to the difficulty of obtaining useful human factors data, that element of the analysis appeared to be the portion of the work still subject to review and potential redirection.

FRA reiterates that the ASCAP approach appears to have significant value for distinguishing risk between the previous condition and proposed systems. However, in developing this final rule, FRA has necessarily taken notice of the fact that constructing the method has proved much more difficult than initially predicted; and nothing approaching validation of the method has yet been undertaken. As a result, the application of recognized alternative risk assessment methods used in other industries is anticipated. These traditional methods will be accepted on a case-by-case basis, after technical review by the Associate Administrator for Safety.

E. Choice of Type of Performance Standard

FRA adopts the performance standard contained in the NPRM, which is basically that the new condition be at least as safe as the previous condition. In the preamble to the proposed rule, FRA acknowledged that this is a static level of safety.

Following issuance of the NPRM, the agency focused further on the problem of how to characterize the base case. FRA noted that, in cases where no adjustment of the previous condition was necessary, the rule might actually result in uneven outcomes depending upon the level of safety on the particular railroad and particular territory. Very often the level of safety is affected significantly by intangibles such as specific provisions of the operating rules, training, degree of supervisory oversight, and degree of professionalism of the work force. A railroad with a good safety record could, in effect, be constrained in terms of future options by its own good performance. Such a railroad would likely have a commitment to continuous improvement, and FRA did not want to create the opportunity for safety to decline. On the other side of the ledger, it is a positive thing that safety would be improved through investments in signals or train control in an area where risk had been relatively higher; however, FRA did not want to ''set the bar too high'' lest needed improvements be discouraged.

FRA embraces this concept of progressive improvement and realizes that actual safety outcomes do differ, despite every attempt to maintain minimum standards. FRA notes that, in cases where adjustment of the base case is required, reliance on average numbers for similar territory may be required, which may have the effect of leveling the playing field over time.

F. Options for Demonstrating Compliance With the Performance Standard

In the NPRM, FRA described a series of options for demonstrating compliance with the performance standard and explained that the option selected could be best described as a Bayesian belief network. A Bayesian Network is a special type of mathematical construct called an ''acyclic directed graph'' that represents relationships between logical propositions consisting of a set of assumptions called variables. A simple example of an ''acyclic directed graph'' is the elimination tree used in many sporting events. Each variable in the logical proposition is independent of other variables that it does not share a common parent with. The joint probability over all variables, which is the probability of the events represented by the graph, occurring is represented in terms of local probabilities associated with each of the individual variables. Its principal limitation is that it may not appear totally objective. It asks that the railroad demonstrate ''to a high degree of confidence,'' that the proposed product would result in no loss of safety. The railroad would be required to make this finding initially. The NPRM attempted to make it clear that, in any case where approval was required, FRA would determine the sufficiency of the safety case. However, the manner in which that would be done was not made clear, since the definition of ''high degree of confidence'' embodied a ''reasonable decision-maker'' standard that would be employed to determine compliance, and the railroad had a duty (carried forward in this final rule) to make an initial determination that the safety case was sufficient.

Since issuance of the NPRM, which pointed out the technical challenges associated with issues underlying administration of a performance standard, FRA has noted slow (albeit demonstrable) progress toward resolution of those issues. Accordingly, FRA is concerned that, given the subjectivity inherent in the ''reasonable decision maker'' finding (which would increase in proportion to the weight of the safety case derived from assumptions and judgments, as opposed to quantified empirical evidence), and given the range of decisions ''reasonable decision-makers'' might make, the proposed structure of the NPRM could prove problematic. In particular, FRA wishes to achieve consistency in outcomes for comparable Product Safety Plans (PSPs), promoting fairness for all parties and predictability in terms of what will be acceptable.

FRA notes that most PSPs will be handled in accordance with the informational filing procedures, and in that context judgments by railroads will be accepted at face value if the necessary analysis has been completed and incorporated into the PSP. However, where FRA is faced with the need to make a decision whether to approve a PSP that is taken for review—given the degree of uncertainty associated with much of the underlying analysis associated with a complex processor-based system—it is important that FRA's judgment be applied. Other provisions of the proposed rule appear to anticipate that this will be done.

Accordingly, in this final rule FRA makes clear that, in any case where approval is required, FRA will make the decision *de novo*, based upon the information provided within or accompanying the PSP and the criteria set forth in § 236.913(g). The result of this change is that any judicial review of FRA's determination would focus on whether FRA came to a result compatible with that of a reasonable decision maker with the agency's expertise and knowledge of its own requirements (by law FRA may not act in an arbitrary or capricious manner), rather than whether the railroad acted as a reasonable decision maker. In any event, given the difficulty of the underlying analysis, it is important for safety and uniformity that suppliers and railroads anticipate the need to make a persuasive case to FRA that the standard is met. FRA also clarifies § 236.909(b) with regard to the finding of sufficiency.

The primary goal of the risk assessment required by this rule is to give an objective measure of the levels of safety risk involved for comparison purposes. As such, FRA believes the focus of the risk assessment ought to be the determination of relative risk levels, rather than absolute risk levels. Thus, like the proposed rule, the final rule attempts to emphasize the determination of relative risk.

The Standards Task Force realized that risk assessments may be performed using a variety of methods, so its recommendation to the Working Group and the Working Group's recommendation to RSAC, in connection with the NPRM, proposed the creation of certain guidelines to be followed when conducting risk assessments. FRA feels that these guidelines, captured in § 236.909(e) and Appendix B, adequately state the objectives and major considerations of any risk assessment it would expect to see submitted per subpart H. FRA also feels that these guidelines allow sufficient flexibility in the conduct of risk assessments, yet provide sufficient uniformity by helping to ensure final results are presented in familiar units of measurement.

One of the major characteristics of a risk assessment is whether it is performed using qualitative methods or quantitative methods. Initially, the Standards Task Force considered proposing that only quantitative risk assessment methods be used to facilitate relative risk comparison. However, suppliers noted that certain risks, such as software coding errors, cannot be fairly or easily quantified, and that the industry practice is to assess such risks qualitatively. As suggested by RSAC at

the NPRM stage of the rulemaking process and as adopted by FRA, the final rule allows both quantitative and qualitative risk assessment methods to be used, as well as combinations of the two. FRA expects that qualitative methods should be used only where appropriate, and only when accompanied by an explanation as to why the particular risk cannot be fairly quantified. RSAC further recommended to FRA (in connection with the NPRM) that railroads/suppliers not be limited in the type of risk assessments they should be allowed to perform to demonstrate compliance with the minimum performance standard. FRA agrees with the philosophy stated here and feels that state of the art of risk assessment methods could potentially change more quickly than the regulatory process will allow, and not taking advantage of these innovations could slow the progress of implementation of safer signal and train control systems. Thus, FRA is allowing risk assessment methods not meeting the guidelines of this rule, so long as it can be demonstrated to the satisfaction of the FRA Associate Administrator for Safety that the risk assessment method used is suitable in the context of the particular product. FRA believes this determination is best left to the FRA Associate Administrator for Safety because the FRA retains authority to ultimately prevent implementation of a system whose PSP does not adequately demonstrate compliance with the performance standard under the final rule.

Regardless of the risk assessment method used, FRA prefers the same method to be used for both previous condition (base case) calculations and calculations of risk associated with the proposed product. FRA prefers similar if not identical methods to be used so that meaningful comparisons can be made. However, the final rule does not mandate that identical methods be used in every case. FRA is aware that some types of risk are more amenable to measurement by using certain methods rather than others because of the type and amount of data available. For example, in almost all situations where advanced train control technology will be economically viable, safety risk data and accident histories will often be more abundant for the previous condition than for operation with the proposed product. The latter calculation will normally be based on supplier data about the product and modeling of how it is intended to be used on the railroad. Because FRA is interested in ensuring that each relative risk determination is accurate, the final rule does not outright mandate that the same assessment method be used. If a railroad does elect to use two different risk assessment methods, FRA will consider this as a factor for PSP approval (see § 236.913(g)). Also, in such cases, when the margin of uncertainty has been inadequately described, FRA will be more likely to require an independent third party assessment (see § 236.913(h)).

VI. Proceedings to Date

On August 10, 2001, FRA published the NPRM concerning the establishment of performance standards for development and use of Processor-Based Signal and Train Control systems (66 FR 42352). As noted above, the NPRM was based on the extensive work of the Standards Task Force and additional input from the entire PTC Working Group. The recommendations of the Working Group, which included those of the Task Force, were recommended by the full RSAC to FRA. Much of the information presented here was published in the NPRM. Since most readers will not have the benefit of consulting both the NPRM and the final rule together, FRA feels that republication of pertinent background and explanatory material in one document is appropriate.

The publication of the NPRM engendered much response. FRA extended the deadline for written comments in response to specific requests for additional time, and to ensure that all commenters had an opportunity to fully develop their observations (66 FR 51362). FRA received a total of 27 comments to the NPRM which can be found in the public docket of the rulemaking. FRA did not receive a request for a hearing and did not hold a hearing.

The comments ranged from observations regarding the historical accuracy of the origin of the practices now codified at part 236 and observations concerning the RSAC process to technical commentary regarding the risk assessment methodology proposed in the rule. The Working Group met December 4–6 of 2001 in San Antonio, Texas to consider comments that had been submitted as of that date. Additional comments were received after the initial Working Group meeting and have also been addressed in this notice. Although the later comments were received long after the deadline for comment submission, FRA has attempted to address those comments, as well.

FRA found the discussions at the December 2001 meeting useful and extremely informative. Many of the commenters were present at the meeting and contributed to the discussion, of comments. Concerns raised by public comments were ultimately resolved by FRA, yet the resolutions were informed by insights obtained in the Working Group discussions. (Minutes of these discussions are in the docket of this rule.) The most challenging issues presented by commenters required additional research and analysis by FRA staff and contractors to the agency.

As noted above, the discussions at San Antonio left open the question of when and how the base case should be adjusted. This issue was pursued by a Working Group team and addressed at the Working Group meeting of July 2003. No consensus on the subject was reached at the 2003 Working Group meeting.

At the July 2003 Working Group meeting, the Working Group did achieve consensus on several recommendations for resolution of other comments on the proposed rule and reported those recommendations to the full RSAC. During August of 2003, the RSAC reviewed the written report of the Working Group and voted by mail ballot. Those recommendations were circulated to the full RSAC for mail ballot, and responses were requested by August 14, 2003. A majority of RSAC members either voted to return the recommendations to the Working Group for reconsideration or non-concurred in the recommendations. Under RSAC procedures, the effect of this vote is to conclude RSAC action on the topic without an RSAC recommendation being to FRA. (Under RSAC procedures, any vote to return consensus recommendations to the working group must be unanimous, or the vote is scored as ''non-concur.'') In any event, FRA's schedule for completion of this rulemaking could not accommodate further months of deliberation on recommendations.

FRA continued to refine the principles of this final rule in light of emerging experience with processor-based systems and risk assessment techniques until the time this final rule was submitted for review and clearance within the Executive Branch in September 2003. FRA has benefitted from the active discussion of the issues in this proceeding, including written comments and deliberations of the RSAC. Although the final resolution of the issues reflects insights gained in discussions of the Working Group and in the NPRM, FRA's final disposition of these issues is the responsibility of the agency and was based on its independent judgment.

The agency is addressing general comments in this introductory portion of the preamble to the rule. However, the majority of the comments are addressed in the section-by-section analysis of the rule text to which they apply.

VII. Comments and Conclusions on General Issues

A. Background and RSAC Process

One commenter wanted to clarify the history of the standards codified in part 236. This comment correctly identifies FRA's predecessor agency, the Interstate Commerce Commission (ICC), as having previously issued the same rules and noted that these regulations were based on the internal rules and practices of various railroads prior to World War II.

Most commenters favorably regarded the RSAC process. One comment suggested continuing the work of the RSAC by developing sample Railroad Safety Program Plans (RSPPs) and PSPs. FRA has decided to continue the work of the Working Group by involving the members in monitoring the Illinois Project and serving as a sounding board for implementation of this rule and for other PTC efforts. Although the work of the group will continue, for reasons discussed later, FRA has determined that the agency will not be involved with the creation of sample documents. A reviewed RSPP draft for the Illinois Project is already available for consideration, and RSPPs are intended to be general documents that may take a similar form on most railroads. This final rule provides a detailed outline of required PSP elements, and the wide variety of products within the scope of the rule will require a range of adaptations in the format and content of PSPs. Other comments probed the membership of the PTC Working Group and inquired about the records kept for meetings and voting. Working Group minutes after publication of the NPRM are available in the public docket. Detailed voting records indicating the way in which various parties voted are not available, since a consensus process was utilized. The Working Group and task forces operated by unanimous consensus, whereby all participants supported the recommendations of the group. This process frequently entailed the presentation of issues and vigorous debate among the four stake holder groups. In many instances, stakeholders advocated opposing views, but were persuaded to either compromise or support the opposite view to attain consensus. The minutes reflect the nature and character of the debate demonstrating various options considered and key points impacting the consensus, when consensus was achieved by the group. The consensus product was then presented to the full RSAC which had the option of accepting or rejecting the Working Group's recommendations by a majority vote. The Working Group reached consensus on the recommendations comprising the NPRM, but could not reach consensus on recommendations for the final rule. Although ballots from the full RSAC are available to the public, these typically only show support or non-concurrence for the final product, not positions on the individual issues that ultimately comprise the final rule. FRA has not kept and therefore has no avenue for providing the voting records on each issue. However, as previously noted, the text of the final rule differs in only a few major respects from the NPRM, which was based on the consensus recommendation of RSAC. In addition, FRA has attempted to note throughout the preamble issues where there were strong discussions and vigorous debate at the working group level.

B. The Performance-Based Approach

FRA has decided to pursue a performance-based standard. FRA did not receive strong comments in support of or against its decision to use a performance-based approach. Comments seem to imply a need for a performance-based approach with some prescriptive elements, in lieu of a pure performance-based approach.

C. The Performance Standard—What Will Be the ''Base Case'' for Comparison?

Among the comments on the risk assessment methodology was a filing from a noted signal expert who faulted the NPRM for, among other things, failing to recognize the capabilities of existing signal technology. The point was that it is incorrect to compare new technology with the rules for older technology (as in the proposed rule's construct for the ''previous condition''), to the extent the rules do not fully mirror that technology's inherent advantages. Rather, the commenter would have FRA recognize the actual capabilities of existing technology built to exceed existing minimum standards in terms of its actual functions. Any other course, it was implied, could lead to a reduction in safety. The commenter cited the example that cab signal systems respond to changes in track occupancy and route conditions almost immediately as an integral characteristic of their design, even though there is no explicit requirement that they do so. By contrast, communication-based technology may experience longer delays in response due to processing time and delays along the communications path. (Note: In FRA's experience, the extent of any difference in time for response to changed conditions may vary significantly from system to system, depending upon the overall architecture of the system, system priorities, communication protocols, communication capacity, and other factors.)

Taking the commenter's point, FRA posed to the Working Group the need to recognize ''best practices'' under traditional signal design principles in constructing any adjusted base case. This resulted in alarm among some members, who viewed the notion as entirely open-ended and as posing the potential that the standard embodied in the rule might become increasingly strict over time. Such a case, they noted, could discourage innovation by holding new systems to an unrealistically high standard based on the existence of little-utilized but theoretically superior technology.

FRA agrees with the commenter that the previous condition should include consideration of the actual functioning of an existing signal technology in place. Indeed, this has never been in dispute with respect to a situation in which no adjustment to the base case is required. Where adjustment to the base case is needed (the contingency most prominent in the commenter's concern), FRA again agrees that the inherent functioning of industry standard technology consistent with subparts A-G of part 236 must be considered in order to avoid the potential for a decline in the actual safety of operations subject to subpart H of part 236.

However, FRA also appreciates the concern that emerged during the December 2001 Working Group discussions that an open-ended standard is not appropriate. Accordingly, FRA wants to make clear that any adjustment should be made using signal technology that is (i) standard practice in the railroad industry (or on the particular railroad, if so desired) as of publication of this final rule and (ii) compliant with subparts A–G of part 236 as amended in this final rule. FRA will accept base case scenarios that utilize this approach, without any attempt to explore what may have been ''best practice'' from some overall industry point of view. Further, the concept of standard technology is one that will be fixed as of a date certain, so ''regulatory creep'' will not occur.

During discussions with the Working Group following the NPRM, it was clear that disagreement existed regarding how best to adjust base case scenarios to accomplish the required risk assessment. Although from time to time it appeared to FRA that differing views reflected in Working Group discussions were converging to produce a clear consensus on a recommendation addressing how to proceed, the problem persisted through the December 2001, 2002, and 2003 Working Group deliberations. Despite FRA's efforts to get full consensus on a recommended resolution to the issue of the adjusted base case, which is admittedly quite complex, the Working Group could not reach consensus on a resolution to recommend to the RSAC on the issue. The Working Group tasked the issue to a team with representation from major stakeholders who met, heard the report of a contractor employed by FRA to review and improve data flows for analysis, considered a report on risk analysis that determined the effect of speed, train density and method of operation on safety risk, and apparently reached agreement on language for approval by the full Working Group. See discussion of § 236.903(e). At the final meeting of the Working Group in July 2003, the group failed to reach consensus on the recommendation proposed by the team. FRA acknowledged the need to resolve the issue on its own. Accordingly, as further detailed in the preamble, FRA has included in the final rule language resolving the issue of ''triggers'' for adjustment of the base case. This language is substantially refined from the general concepts embodied in the NPRM and should provide very objective guidance regarding the circumstances under which the base case must be adjusted.

At the Working Group meeting in December 2001, it also became clear that the issue of train control, as opposed to signal technology, presents a special problem. The regulatory structure for train control is essentially unchanged from issuance of the ICC's RS&I in 1937. The RS&I had its roots in ICC orders beginning in 1922, and since FRA's creation in 1967, the RS&I has been carried forward in part 236.

Realistically, for operations in excess of 79 mph (see § 236.0) FRA applies the current regulations only to existing systems. Existing systems have not been extended to additional territories in part because of the costs involved. Identified safety needs have been addressed by FRA orders. For instance, following the Chase, Maryland, collision of January 4, 1987, FRA was required by law to order installation of speed control (ATC) on all freight and commuter trains operating on the Northeast Corridor (NEC), complementing the cab signal systems already in use. Section 9, Public Law 100–342; 52 FR 44510 (Nov. 19, 1987); 53 FR 1433 (Jan. 9, 1988); 53 FR 39834 (Oct. 12, 1988). As higher speed operations came to the NEC and European signal technology provided the opportunity to achieve full PTC functions, FRA required installation of the ACSES on initial territories, noting the potential for application corridor-wide at an appropriate time. 63 FR 39343 (July 22, 1998).

When Amtrak planned higher speed operations on its Michigan line, FRA supported installation of the Incremental Train Control System (ITCS), providing a limited waiver for system characteristics that differ from traditional signaling technology. ITCS provides positive stop capability as well as speed control and can be utilized to protect work zones. Although a commenter in this proceeding questioned whether ITCS provides the same level of safety as a cab-signal based system, there can be no doubt that it far exceeds the safety provided by an intermittent train stop system. In summary, while existing rules still apply to existing systems, new higher speed operations have been subjected to higher standards.

During Working Group discussions following issuance of the NPRM, FRA considered providing generic guidance for construction of adjusted base cases for PSPs involving planned speeds that exceed 79 mph. FRA further considered participating in consultation with respect to the appropriateness of alternative approaches, based upon the facts in particular cases. FRA has concluded such guidance is necessary and has provided that guidance in the final rule. Of course, FRA cannot relinquish its responsibility ultimately to determine whether the performance standard has been met. In order to provide meaningful flexibility to utilize approaches grounded in systems now in use, optimizing use of public and private resources, FRA is prepared to consider use of base cases employing cab signals and continuous train stop, where that is commercially and operationally realistic and within a reasonable speed range. FRA does not believe that the allowance in existing regulations for intermittent train stop technology would be appropriate for extension to the new performance-based rule. While that technology has an acceptable record under existing conditions of operations, it deviates from the fail-safe requirements applicable to other signal and train control systems and has clear vulnerabilities that have been realized in practice. By the same token, consideration of systems exceeding ACS/ATC is appropriate where train speeds exceed 110 mph, based on determinations FRA has made concerning the NEC, as noted above.

Accordingly, the guidance for adjustment of base cases that is set forth in § 236.909(e) of this final rule also addresses cases involving higher speed operations. In that guidance, FRA emphasizes that high speed rail passenger service should be supported by highly competent train control technology. In view of safety concerns attendant to passenger service and the fact that much of the cost of rail passenger service is met out of public sources, FRA will, where appropriate, examine new high speed passenger rail projects and propose appropriate orders setting a floor for safety for the new systems.

With respect to the base case for the NAJPTC problem, FRA indicated a willingness to make a provisional decision on revenue service for the Illinois PTC system based upon the risk assessment approach described above. Given the configuration of that system and the scope of operations involved, FRA believes that the information under development should be sufficient to permit FRA to estimate whether the PTC system is fully adequate from a safety point of view, particularly as to the fixed block operations planned for revenue service. FRA will make available funding for a required follow-on assessment, utilizing ACS/ATC as the method of operation, so that a more complete and precise record is available to guide deployment of that technology elsewhere on the national rail system. This is particularly important because the project goals include demonstration of (i) ''moving'' block operations which was not contemplated by previous rules and (ii) provisions for ''non-communicating'' (unequipped) trains, which was contemplated but not allowed by previous rules.

D. How Does This Rule Affect Locomotive Electronics and Train Control?

The earliest train control systems were electro-mechanical systems that were independent of the discrete pneumatic and mechanical control systems used by the locomotive engineer for normal throttle and braking functions. Examples of these train control systems included cab signals and ACS/ATC appliances. These systems included a separate antenna for

interfacing with the track circuit or inductive devices on the wayside. Their power supply and control logic were separate from other locomotive functions, and the cab signals were displayed from a separate special-purpose unit. Penalty brake applications by the train control system bypassed the locomotive pneumatic and mechanical control systems to directly operate a valve that accomplished a service reduction of brake pipe pressure and application of the brakes as well as reduction in locomotive tractive power. In keeping with this physical and functional separation, train control equipment on board a locomotive came under part 236, rather than the locomotive inspection requirements of part 229. Systems of this type remain in service, and FRA regulations arguably continue to require this type of functional separation in the absence of a waiver or order applicable to the particular technology (see, *e.g.*, 49 CFR §§ 236.5, 236.507, 236.516).

Nevertheless, as the price of microprocessors decreased, and their capability increased, the original equipment manufactures (OEMs) of the various components making up the locomotive and the train control systems began individually repackaging the individual components using the enhanced microprocessor capabilities and eliminating parts and system function control points access. Access to control functions became increasingly restricted to the processor interfaces using proprietary software. While this resulted in significant simplification of the previously complex discrete pneumatic and mechanical control train and locomotive control systems into fewer, more compact and reliable devices, it also eliminated many of the parallel independent control paths previously available to train and locomotive control systems. For example, in the case of pneumatic and mechanical brake system components, the introduction of electronic air brake controllers resulted in the elimination of the mechanical valve previously used for penalty brake applications by the train control system. As a result, penalty application of brakes by the once isolated, totally segregated train control systems could now only occur if the air brakes were actuated through the locomotive electronic air brake controller.

The OEMs also began tapping certain inputs or outputs of the proprietary systems of the individual components for locomotive information. Individual gages displaying operating parameters (such as speed, brake pipe pressure, and amperage) to the engineer were replaced by single integrated electronic displays. These new microprocessor controlled locomotives now respond to operator commands, display system status, and simultaneously make numerous automatic adjustments to locomotive systems to ensure efficient operation. These new locomotive electronic controls, while designed with a high degree of attention to safety, have been built to different design standards and requirements than train control systems and have thus far not been demonstrated to fail safely. In individual cases unsafe failures have occurred. In effect, electronic control of locomotive functions has arisen in recent years without the same degree of regulation as train control functions, and in some cases products have been deployed prior to a level of analysis and testing that would be considered acceptable in a train control system. As a result, locomotive engineers have expressed concern regarding the safety characteristics of certain electronic features. Despite the best efforts of OEMs and suppliers, in some cases engineers have been relegated to use of emergency brake valves in the face of blank screens and uncertain availability of normal control functions.

FRA asked for comment on this issue. GE Transportation Systems responded requesting only that train control circuitry be clearly distinguished from locomotive electronics. GM Electro-Motive (EMD) did not respond until December of 2002, long after the official close of the comment period. EMD asked that the preamble discussion on integration of functions be stricken. EMD felt that requiring isolation of train control functions could drive up costs and slow adoption of PTC. EMD noted that many of the components and subsystems required for PTC are already on board today's locomotives (*e.g.*, power supplies, GPS, displays, data radios). EMD went on to say that in-service failures should be handled in a fail-safe manner, without any operator intervention. EMD continued ''the precise mechanism for handling in-service failures is dependent upon the system architecture and must be addressed uniquely by the Product Safety Plan.'' Further, EMD suggested that ''partitioning and de-coupling strategies should be used to execute train control functions on the locomotive platform, thereby avoiding subjecting the entire locomotive electronics suite from falling within subpart H of part 236.''

Locomotive manufacturers can certainly provide secure locomotive and train controls, and it is important that they do so if locomotives are to function safely in their normal service environment. FRA highly encourages the long-term goal of common platform integration.

As noted in the NPRM, this rule is being prepared against a background of rapid and significant change in locomotive design. This change has direct implications for the future of both train control and locomotive control systems on board locomotives. The net result has been a merging of systems designed to different regulatory standards with differing levels of safety analysis at a single point.

This final rule does not preclude the integration of functions if the overall safety case is made with the required high degree of confidence. It should be noted that for new locomotives in passenger service, 49 CFR ''§ 238.105 establishes requirements for fail-safe characteristics or safety redundancy for braking and power functions that are electronically controlled. In the near future, FRA expects to explore further the need for safety criteria for critical locomotive control functions in both passenger and freight service.

VIII. Section-by-Section Analysis

Section 209.11 Request for Confidential Treatment

FRA is amending this section, as proposed in the NPRM, to clarify existing procedures for requesting confidential treatment for documents provided to the FRA in connection with the agency's enforcement activities. The Standards Task Force was concerned that confidential documents would need to be provided to FRA under parts 234 and 236, and that FRA needed to clearly indicate that it would protect such documents. The NPRM proposed to address this issue by amending paragraph (a) of § 209.11 to indicate that the procedures governing requests for confidential treatment apply to documents provided to the FRA in connection with the agency's enforcement of both the railroad safety statutes and the railroad safety implementing regulations.

FRA received several comments on this section. One commenter suggested that no information submitted to the FRA should be treated as confidential. FRA disagrees, and notes that the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Trade Secrets Act (18 U.S.C. 1905) protect confidential information from public disclosure. Another commenter suggested that FRA confirm that information will be accorded confidential treatment. FRA cannot make any flat pronouncements about the confidentiality of information

it has not yet received. However, it is likely that the type of proprietary information to be submitted in compliance with this rule may be withheld from release as a trade secret or commercial or financial information covered under exemption 4 of the FOIA. It is not the policy of FRA to publicly disseminate such information as will be submitted in compliance with this rule. Should a FOIA request be made for information submitted under this rule, the submitting company will be notified of the request in accordance with the submitter consultation provisions of the Department's FOIA regulations (§ 7.17) and will be afforded the opportunity to submit detailed written objections to the release of information protected by exemption 4 as provided for in § 7.17(a). Because there is no public disclosure requirement in this rule, there is no need at this time to substantially revise § 209.11, but FRA intends to review its confidential business information regulations in the near future.

Section 234.275 Processor-Based Systems

Section 234.275 contains standards for highway-rail grade crossing warning systems using new or novel technology or providing safety-critical data to any product governed by subpart H of part 236. Currently part 234 provides requirements for the maintenance, inspection, and testing of highway-rail grade crossing warning systems. In September 1994, FRA issued a final rule on part 234 (Grade Crossing Signal System Safety, 59 FR 50,086, Sep. 30, 1994), but the final rule did not address processor-based warning systems which are integrated with signal and train control systems. FRA felt it was necessary for these types of systems to be addressed in subpart H because of the potential for their integration or interaction with processor-based signal and train control systems. With the large number of processor-based warning systems currently installed at the nation's highway-rail grade crossings, however, it would be unrealistic to attempt to bring all of those within the scope of subpart H. The processor-based warning systems currently in use and meeting the maintenance, inspection, and testing requirements of part 234 do an admirable job of warning highway users. The Standards Task Force formed a team of its members (prior to publication of the NPRM) to identify such items as PTC system data to be transmitted to and integrated with highway traffic control/information systems (future capability). See ''Implementation of Positive Train Control Systems,'' page viii (September 8, 1999). The team's focus captured the potential uses of Intelligent Transportation System (ITS) technology at highway-rail grade crossings. This section identifies which processor-based highway-rail grade crossing warning systems are subject to the requirements of subpart H of part 236.

Paragraph (a) provides that relevant definitions of part 236, subpart H, apply to this section.

Paragraph (b) provides a standard for whether a highway-rail grade crossing warning system must meet the requirements of subpart H. ''New or novel technology'' is defined in the third sentence of the paragraph. FRA envisions new or novel technology to include such technology as that incorporated in new designs which do not use conventional track circuits. For instance, ITS contemplates intelligent controllers that utilize data provided through advanced signal and train control systems to warn motor vehicle drivers of approaching trains. FRA does not intend for new or novel technology to include any technology used in current systems (as of the effective date of this rule), which is consistent with the approach recommended by the Standards Task Force for the NPRM.

Paragraph (c) contains requirements for equipment subject to this section. These are additional requirements which must be included in the PSP.

Paragraph (d)(1) confirms that this section in no way authorizes deviation from the requirements of the Federal Highway Administration's Manual for Uniform Traffic Control Devices (MUTCD). Current ''wayside'' warning devices are standardized by the MUTCD. The MUTCD sets forth the basic principles that govern the design and usage of traffic control devices for all streets and highways open to public travel regardless of type of class or the governmental agency having jurisdiction. Part VIII of the MUTCD applies to traffic control systems for highway-rail grade crossings. Traffic control systems for such crossings include all signs, signals, markings and illumination devices along highways approaching and at crossings. Traffic control systems are required to be consistent with the design and application of the standards contained within the MUTCD.

FRA received one comment generally supporting this section. The commenter concurred with the language proposed in the NPRM for this section as necessary to ensure the safety and integrity of the system throughout its life cycle.

Section 236.0 Application, Minimum Requirements, and Penalties

As a general matter, this final rule applies to all railroads, with two exceptions. First, railroads which operate only on track that is not part of the general railroad system of transportation are excepted from all requirements of part 236. Second, rapid transit operations in an urban area which are not connected to the general railroad system of transportation are unaffected by the requirements of part 236. FRA changed this language solely to standardize the application of all of the Federal regulations related to railroad safety. For additional information on the extent and exercise of FRA's safety jurisdiction, see 49 CFR part 209 Appendix A as amended on July 10, 2000 (65 FR 42544).

FRA also added a provision noting that a person may be subject to criminal penalties for violating the provisions of 49 U.S.C. 21311. FRA has similar provisions in its other regulations requiring persons or entities to report information to FRA for safety data purposes. FRA's intention here is to emphasize the importance of truthful recordkeeping and reporting, and the possible penalties for failure to do so.

Section 236.18 Software Management Control

This section requires that all railroads adopt a software management control plan to assure that software used in processor-based signal and train control equipment in service is the version intended by the railroad to be in service at each location. Simply put, a software management control plan is an inventory of software at each equipment location. As a processor-based signal and train control system ages and experiences modifications (i.e., changing operating conditions or upgrades in hardware and software), the software management control plan should be updated accordingly, providing traceability to previous versions of software. One should always be able to determine from the software management control plan precisely what software is installed at each equipment location in the field. This requirement provides an audit trail to determine if the correct software is installed at the correct locations for all processor-based signal and train control systems on a railroad.

FRA is requiring this plan because for a considerable time after the introduction to the railroad industry of processor-based equipment in signaling systems, components of such systems were not handled responsibly. It was

not unusual for railroad employees to carry in their clothing pockets printed circuit (PC) boards and the programmable memory devices (PROMS) which plug into those boards. When troubleshooting a piece of equipment, it was common practice to simply exchange the failed PC board with ones from the selection the employee had on hand until the device appeared to function as intended. The pulled board was often saved for the purpose that it might work in another device. For this and other reasons, in the Orders of Particular Applicability for processor-based train control systems on the NEC (63 FR 39343, 52 FR 44510), PROMS were required to be soldered in place in order to assure proper software versions were installed on locomotives. FRA has addressed these practices with railroads where they have been detected, but some no doubt continue to the present day.

With the proliferation of processor-based equipment and use of PROMS with both erasable and non-erasable memory, it is no longer practical to require the soldering of PROMS on PC boards. A software management plan will track the version of software which should be and is in use at all equipment locations on a signal and train control system. Therefore, a requirement for software management control plans provides adequate assurance that processor-based equipment is programmed with the correct software version.

The inventory should identify, among other things, the software by version number. FRA expects the software management control plan to identify and document for each equipment location the executive or application software name, software version number, software revision number, date of software revision, and a description of the cyclic redundancy check for verifying PROM contents. Prior to the issuance of the NPRM, the Task Force had initially considered a requirement that railroads adopt configuration management plans for existing systems, which would cover both software and hardware dealing with safety-critical aspects of processor-based signal and train control systems. Railroads expressed concern during discussions of the Working Group that such a requirement would be unduly burdensome since there is no current configuration management requirement in place, and that certainly simple one-for-one hardware changes need not be tracked. As a practical matter, FRA envisions a limited amount of hardware tracking as a necessary element of software management, since software can reside in portable hardware elements. FRA invited comment on this issue in the NPRM and received several in favor of requiring a hardware and software management control plan. These comments expressly stated that hardware tracking is a necessary element of software management. As previously noted, the subject of configuration management was contemplated by the Standards Task Force (pre-NPRM), but the group opted to recommend to the Working Group that the tracking for existing systems be limited to a software management plan. RSAC made the sure recommendation to FRA, which FRA embodied in the NPRM. FRA has noted the concerns of commenters, but FRA agrees with the decision of the Standards Task Force, pursuant to the reasoning articulated above about the undue burden such a provision would entail, not to include hardware in the software management control plan.

There is currently no recognized industry standard for software management; however FRA is aware that other computerized systems on railroads such as accounting and communications systems use configuration management control principles. FRA believes that a requirement for software management control plans on signal and train control equipment will enhance the safety of these systems and ultimately provide other benefits to the railroad as well.

Under this section, railroads are responsible for all changes to the software configuration of their products in use, including both changes resulting from maintenance and engineering control changes, which result from manufacturer modifications to the product. In FRA's view, both of these types of changes carry significant safety implications, and should be tracked by the railroad. FRA is aware that most maintenance changes involve replacement of PC boards or software on PROMS, and that changes such as replacement of resistors on PC boards are not normally made by the railroad, but rather the product manufacturer. FRA feels that it would be appropriate for the railroad to track changes no deeper than at the PROM software levels; however, it would be unrealistic and cumbersome to expect the railroad to document changes such as replacement of resistors on PC boards.

The NPRM recognized that the proposed section imposed a strict liability standard on the railroads regardless of culpability, and that railroads may be penalized in situations where they receive inaccurate information from the product manufacturer concerning manufacturer modifications which may pose a safety risk. While railroads should be entitled to rely on the manufacturers' product information, since manufacturers obviously know much more about the specifics of their products, FRA intended to hold the railroads responsible since they are primarily responsible for the safety of their operations. On the other hand, a supplier that provide inaccurate information or provides information in an untimely way would cause the railroad to be in violation of its obligation to implement a plan that contains current and accurate information. Under § 236.0(f), any person that causes a violation of part 236 is liable for a civil penalty. With regard to PSPs, the final rule requires that the railroad disclose contractual relationships with the software supplier to ensure such timely notification of safety critical changes. See § 236.907(c)(3). Product suppliers entering into contractual arrangements for product support described in a PSP must promptly report any safety-relevant failures and previously unidentified hazards to each railroad using the product. See § 236.907(c)(4).

FRA invited comments addressing the issue of whether railroads and suppliers ought to share responsibility for the duty of maintaining proper software configuration, and if so, how such responsibility can be effectively delineated. FRA received comments suggesting that the supplier should be responsible for supplying initial software configuration information with the exception of embedded proprietary software and provide software configuration information for changes impacting safety. Another commenter provided a more detailed scenario for assigning responsibility where the suppliers providing the product directly to the railroad would be responsible for verifying the safety of the executive software and the version control of that software. The software version control would clearly identify safety related changes, required supporting hardware, and the compatible interfaces. The railroad would be responsible for maintaining version control of site specific application software for products or systems, and verify the compatibility of all component interfaces.

FRA clearly intends to hold railroads responsible as they are primarily responsible for the safety of their operations, but recognizes the extreme importance to be accorded the supplier or manufacturer. In fact, FRA acknowledged the importance of the

manufacturer's role to the process by inviting comments on the scope of a product manufacturer's duty to provide accurate information concerning initial software configuration of its products and any engineering control changes and the railroads' ability to rely on the information provided by the supplier. FRA received no comments addressing this duty of accuracy by the manufacturer. FRA did however receive a comment generally addressing inclusion of processes to ensure proper configurations. See, also, discussion of § 236.907(c)(3).

Paragraph (a) of § 236.18 discusses the application of this requirement to all railroads within 6 months of the date that the final rule is published and also discusses how it applies to railroads not in operation as of the effective date of this rule. FRA intends for this requirement to apply to all systems which would be specifically excluded by § 236.911 in subpart H. For subpart H products, configuration management for each product must be specified in the PSP and the Operations and Maintenance Manual, as required by §§ 236.907(a)(13) and 236.919(b). These specifications must comply with the railroad's RSPP.

Although the issue of allowing time for compliance was not covered by the Standards Task Force, FRA proposed a 24-month time period as sufficient. FRA sought comment on this issue and received comments both in support and against the proposed 24 months. Comments seeking more time concluded that a 24-month period may not be sufficient due to the significant impact on the development processes, documentation requirements, and product development cycle for products already being designed. The Working Group favorably discussed recommending 30 months for implementation of the software management plan following its completion. Of course, the full RSAC did not make consensus recommendations to FRA on how to resolve comments on the NPRM. Nevertheless, FRA is persuaded by the rationale suggesting the need for extension of the implementation period. FRA has decided to change the language from the NPRM to allow a longer implementation period. In essence, the change extends the previously proposed period of 24 months to 36 months, with 6 months allowed to develop and adopt the plan and 30 months allowed to implement it.

Paragraph (c) replaces the language originally proposed as paragraph (b). FRA received a comment stressing the need to revise the language to require a description of the process to ensure proper configuration in lieu of the previous language which required the identification of the actual testing procedures used to confirm proper configuration. The commenter appropriately distinguished the testing procedures which would be tailored to a particular product from the overall process which could be applied to numerous products. FRA agrees with this distinction and has incorporated the suggested change. As revised, the paragraph requires software management control plans, and further requires that the plan describe the process for identifying and confirming proper configuration when any type of change occurs.

Section 236.110 Results of Tests

FRA is modifying existing § 236.110 to include record keeping requirements for processor-based signal and train control systems under part 236, subpart H, and to make it consistent with current agency policy concerning record keeping. As modified, § 236.110 would incorporate in four paragraphs new language and language from current § 236.110.

Paragraph (a) outlines four primary changes. First, FRA is adding a new section to the list of sections to which § 236.110 applies: § 236.917(a), applies to processor-based equipment covered by subpart H. Currently, there is no established safety record or performance history for these new types of systems.

Second, paragraph (a) allows for electronic record keeping. This policy is consistent with FRA's policy of encouraging electronic record keeping. FRA is requiring that carriers adopting electronic means to record results of tests first obtain FRA's approval through an application process. Requiring FRA approval will establish a process whereby FRA can ensure all the proper information (prescribed in proposed paragraph (a)) is recorded. FRA will also be able to determine where and how the electronic records are available for inspection. FRA notes that if tests are performed by Automated Test Equipment (ATE), the test equipment shall be identified by a unique number, and the test record must reflect that number.

Third, FRA is changing § 236.110 to make clear that records filed with a railroad supervisory officer with jurisdiction are subject to inspection and replication by FRA and FRA certified state inspectors. Railroad supervisory officer is intended to mean an assistant signal supervisor, signal supervisor, or any responsible divisional officer. If a railroad receives approval for electronic record keeping, the railroad shall inform FRA how and where the electronic records will be available for inspection during normal business hours. However, in the case of life cycle records required by proposed § 236.110 (c) (1), the railroad shall inform FRA of the office location(s) where these life cycle records will be kept. If electronic record keeping (in accordance with paragraph (e)) is not used for train control test records, then these records must be kept at the locomotive office nearest the test point location(s).

Fourth, paragraph (a) corrects a misprint in current § 236.110, concerning the list of sections to which it applies. The paragraph lists in proper numerical order the sections to which § 236.110 applies.

Paragraphs (b), (c), and (d) provide requirements for how long such records specified in paragraph (a) are to be maintained. Paragraph (b) simply restates a current requirement of § 236.110 (fourth sentence).

Paragraph (c) provides a requirement specifying the length of time records made in compliance with § 236.917(a) are to be kept. Paragraph (c)(1) requires that all railroads maintain records for results of tests conducted when a processor-based signal or train control system is installed or modified. These records must be retained for the life cycle of the equipment. FRA feels tracking modifications to processor-based equipment is necessary, because such changes, especially those concerning software, are not often readily apparent, yet may lead to hazardous conditions. Whenever processor-based equipment or software is modified or revised, it must be tested to ensure it is still functioning as intended. FRA believes these records will also provide valuable information to the railroad and manufacturer pertaining to the reliability of the equipment.

Paragraph (c)(2) deals with maintenance and repair records. The NPRM proposed requiring the records to be maintained for one year, or until the next record is made. There were two reasons for this requirement. First, a subset of these records (those involving hazardous events) will be tracked in the product's hazard log (see § 236.907(a)(6)). Second, many repairs to signal and train control equipment are not performed by the railroad, but rather by contractors. It would be burdensome for repair records to be tracked by the railroad for the lifetime of the product when different contractors might be performing the actual repair work over the product's

lifetime. Thus, a requirement for lifetime record retention of test records pertaining to product repairs would be substantially duplicative and burdensome. However, FRA has noted that PSPs should address issues of railroad signal employee access to repair records and hazard logs for products used throughout the railroad, as these may contain important information for performance of their duties.

Paragraph (d) simply restates a current requirement of § 236.110 (fifth sentence).

Paragraph (e) allows electronic recordkeeping in lieu of preprinted paper forms.

Section 236.787a. Railroad

FRA inserted this definition to aid in standardizing the application provisions of its regulations.

Section 236.901 Purpose and Scope

This section describes both the purpose and the scope of subpart H.

Section 236.903 Definitions

FRA received a number of comments suggesting new definitions, as well as comments addressing various definitions included in the NPRM. Among the comments suggesting new definitions was a recommendation that the final rule include a definition for the term ''application software.'' The commenter, however, did not propose a definition for consideration by the agency. Although the comment was considered, FRA could not recommend a definition for the term that would provide clarity to the concept.

Other commenters requested the term ''train control'' be defined in the rule. FRA received two suggestions for definitions of train control. One definition stated,

> Train control means the primary system that instructs the train operator or other track occupant on speed or authority limits and/or automatically restricts the train or other vehicle to the speed or authority limit.

The other suggested definition stated,

> Train control is a part of a system interlinked from wayside to track vehicle that automatically warns and enforces against violation of track speeds and authority limits.

The underlying concern presented by these commenters is to ensure the final rule is not misconstrued to cover systems that are not train control systems. The commenters stress the distinction between systems that can initiate enforcement and actually control the train and systems that merely provide information to those individuals controlling the train. In particular, the commenters do not want train pacing systems, alerters and End of Train Devices (EOTs) considered train control systems for purposes of this rule.

FRA agrees and realizes that historically, there was an understanding among parties in the railroad industry regarding what constitutes a train control system. FRA further recognizes that evolving technology will change the nature of what is traditionally considered train control. FRA has decided that an attempt to craft a clear definition or even a laundry list of what systems or features are considered train control or components of train control systems may actually confuse the issue. Since the technology supporting these systems is continuously evolving any list would undoubtedly be outdated at its inception or shortly thereafter. The purpose and scope provision of this rule found at § 236.901 clearly limits the rules application to ''safety critical products.'' FRA believes the definition of ''safety critical'' excludes systems that merely provide information. In lieu of attempting to craft a definition of train control, FRA has clearly articulated that pacing systems, alerters, and EOTs are not train control systems, which appears to address the immediate concern of these comments. Having satisfied the immediate concerns and given the difficulty of crafting a definition, FRA has decided to leave the term ''train control'' undefined.

''Train control'' is, among other things, a statutory term; and FRA is keenly aware that evolving electronic architectures will present a variety of questions with respect to the applicability of subpart H. FRA believes these challenges should be considered on their merits, rather than through adoption in the present proceeding of a definition that is over- or under-inclusive.

In the definition of ''safety-critical,'' FRA has already said that the reach of this proceeding extends to systems that are overlaid on existing methods of operations without being integrated into those systems. Such systems monitor compliance and intervene as necessary to prevent accidents and casualties, and in the future some existing signal systems may be removed because of the safety net they will provide. Other systems providing safety-relevant information on which crews are expected to rely will also fall within this term.

In particular, FRA wishes to emphasize that systems that deliver mandatory directives in text or graphic format are also train control systems. These systems have been excepted from part 220 (Radio Communications) specifically because it was understood that special attention would need to be given to the safety and security of such systems. In light of the events of September 11, 2001, it is particularly important that oversight be provided for implementation of these systems (which FRA encourages and will seek to facilitate).

In referring to overlay systems and systems for the digital transmission of mandatory directives as train control systems, FRA recognizes the reality that both safety and operational efficiency will almost inevitably be implicated in these new technologies. Communications capability will be relied upon to move trains more efficiently, and more or less subtle changes to the underlying methods of operation will emerge. Employees will come to rely on information provided by the systems (including negative cues garnered from the lack of intervention). FRA does not object to these changes, but it is important that the changes be summed into a PSP for analysis so that pluses and minuses can be accounted for and the overall safety impact of the changes can be evaluated.

In addition to suggestions for new definitions, comments were submitted addressing various definitions proposed in the NPRM. These comments will be discussed with the corresponding explanation of each term.

The term ''component'' is intended to signify an identifiable part of a larger program or construction. A component usually provides a particular function or group of related functions. By requiring such a definition, FRA does not intend to overburden railroads or suppliers by requiring safety performance data and analysis on the least significant of these identifiable parts. Rather, FRA encourages railroads to take advantage of supplier data, which is normally readily available for off-the-shelf components. FRA assumes that railroads and suppliers will use discretion to appropriately define components at levels not quite as simple as a resistor, but also not quite so complex that they could not be readily replaced. For instance, FRA envisions components defined no more specifically than at the printed circuit board level, or E–PROM level.

FRA has added a definition of the term ''employer.'' The term employer means a railroad, or a contractor to a railroad, that directly employs or compensates individuals to perform the duties specified in § 236.921(a). This definition is needed as a result of the change in the language of § 236.921 to make clear that railroad contractors, as well as the railroads are responsible for

training their employees performing the work specified in § 236.921(a).

The term ''executive software'' is intended to encompass that software which affects the overall structure of a signal or train control system and the nature of the interfaces between its various subsystems and components. Executive software typically remains the same from installation to installation; the design is not changed and it is not recompiled. Executive software only changes when the manufacturer issues a revision or new version/upgrade.

The term ''full automatic operation'' is defined per recommendation from the Standards Task Force. This definition was crafted with respect to the railroad industry, which involves both freight and passenger operations. Other definitions come from the transit industry and involve such nuances as door control. The definition captures the notion that locomotive engineers/operators may act as both passive monitors and active controllers in an full automatic operating mode.

This rule is not designed to address all of the various safety issues which would accompany full automatic operation. Indeed, FRA would anticipate the need for further rulemaking to address the wide range of issues that would be presented should automatic operation be seriously contemplated. However, insofar as skills maintenance of the operator is concerned, the rule offers standards in § 236.927.

The term ''high degree of confidence'' was defined in the NPRM to mean ''there exists credible safety analysis which is sufficient to persuade a reasonable decision-maker that the likelihood of the proposed condition associated with the new product being less safe than the previous condition is very small (remote).'' This proposed definition was addressed by several commenters, who concluded that the term was subjective, but provided no alternative suggestion. One commenter acknowledged there is no standard that would not be subjective and noted that they could live with the inherent subjectivity of the term and concept. FRA, however, found the term's application inappropriate for subsystem and component level estimates. FRA is therefore changing the definition proposed in the NPRM to indicate that the term is to apply only at the highest level of aggregation of processor based components. FRA received one final comment addressing this term, contending the parenthetical at the end of the definition ''(remote)'' does not enhance or provide clarity to the concept. The word ''small'' is already used within the definition and needs no further explanation. In addition the word ''remote'' may actually add confusion instead of clarity as it has a specific meaning in the risk assessment area. FRA is changing the proposed definition by striking the parenthetical. Further, for reasons detailed above under the discussion of the performance standard, FRA is removing the language concerning the ''reasonable decision-maker.'' The final definition reads as follows:

High degree of confidence, as applied to the highest level of aggregation, means there exists credible safety analysis supporting the conclusion that the likelihood of the proposed condition associated with the new product being less safe than the previous condition is very small.

The term ''human factors'' refers to the limitations in human performance, abilities, and characteristics that designers should consider when designing subpart H products. FRA believes that designers can improve the safety of products by considering human factors as early as possible in the design process. Design that does not account for human factors, however, can degrade safety.

The term ''human-machine interface'' refers to the way an operator interacts with the product. FRA feels designers who incorporate human factors design principles in a human-machine interface can increase system safety and performance.

The term ''Mean Time to Hazardous Event'' (MTTHE) is used to capture the parameter widely accepted in the safety/reliability engineering discipline as a scientifically based prediction of the measure of time likely to pass before the occurrence of a hazardous event. Railroads have indicated objection to the use of the term ''average'' or ''expected'' in the definition of MTTHE. FRA invited comment on this specific issue. FRA received comments generally in favor of the use of the words ''average'' or ''expected'' in the definition. Other comments addressed the term MTTHE generally. One commenter considered the concept of a mean time to a potential hazard troublesome, arguing that if a potential hazard is recognized it should be fixed. This concern and others are not likely to be addressed by a change in the definition and will be discussed with comments on the risk assessment. Another commenter objected to the use of MTTHE as confusing when there is already a commonly used term ''Mean Time Between Hazardous Events'' (MTBHE) that captures the concept. The commenter encouraged consideration of the IEEE definition of MTBHE to prevent confusion and encourage consistency, yet seemed comfortable with the other term and expressed no objection to the use of the words ''average'' or ''expected'' as part of the MTTHE definition. FRA believes the difference between the terms MTTHE and MTBHE is minor, and renders similar if not identical numerical values. The latter implies there has been a previous hazardous event and provides an exponential number representing some unit of time (*e.g.* years or hours) before another hazardous event occurs. Similarly, MTTHE assumes that no hazardous event has occurred and provides an exponential number representing some unit of time before the first hazardous event occurs. In either case, the number represents the average time before a component, subsystem or system failure. FRA believes that it is more appropriate to use MTTHE in light of the gravity of a railroad hazardous event, which may entail consequences that include complete loss of railroad infrastructure or even human life. FRA adopted and does not intend to change the MTTHE as a pro-active measure, which does not assume repetitive hazardous events.

The term ''new or next-generation train control system'' is intended to capture the notion of a train control system utilizing a relatively new technology or new generation of technology, not currently in use in revenue service. Under this definition, a significant change in the way signal and train control systems work, such as that brought about by Locomotive Speed Limiter (LSL), could trigger classification as a new or next-generation train control system. Other factors, such as the relative maturity of the product brought to market, may be relevant to this determination.

The term ''predefined change'' is intended to signify any change likely to have an effect on the risk assessment for the product. FRA imagines that predefined changes will include: Additions, removals, or other changes in hardware, software, or firmware to safety-critical products, application software, or physical configuration description data, under circumstances capable of being anticipated when the initial PSP is developed. FRA wants to clarify that these changes would include not only changes made directly to the product, but changes in the product's use.

FRA urges parties developing PSPs to consider all likely configurations for the product, and include such considerations in the risk assessment. This will reduce the likelihood of being

required to file a PSP amendment at a later date when the railroad wishes to slightly reconfigure their product or make a slight change to it.

The term ''preliminary safety analysis'' is intended to signify the process used to develop a comprehensive listing of all safety-enhancing or safety-preserving functions which safety-critical products will perform. This listing should address the requirements currently used to provide for safety of train movements in the RS&I (part 236). It should also be consistent with those requirements derived from laws of physics, such as minimum required braking distances, and provide guidance as to how such requirements should be met. FRA received one comment indicating that the term is mistakenly listed as ''preliminary safety analysis'' in the definition section as well as in the rule text. FRA understands that the term preliminary hazard analysis is a more common term in system safety work, but the usage in § 236.905(b) connotes a much broader scope of inquiry. Accordingly, while the term is far from ideal for this application, it has been carried forward as proposed. (The term ''preliminary hazard analysis'' (PHA) refers to a discrete step in the safety assessment process (specifically verification and validation) that follows or is performed in conjunction with the initial description of system requirements and leads to the creation of a hazard log. Although the term is not used in the PSP section of the rule, a PHA will typically be performed as part of the PSP development process.)

The term ''product'' is intended to encompass all signal or train control equipment which is processor-based, including: (i) A processor-based component of a signal or train control system, and (ii) a processor-based subsystem of a signal or train control system, or (iii) the system itself, if processor-based.

The term ''safety-critical'' is intended to apply to any function or system the correct performance of which is essential to the safety of personnel and/or equipment, or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist. An example of the latter would be an ''overlay'' system that does not constitute any part of the method of operation, but maintains safe system operation should any one of the safety-critical functions be omitted or not performed correctly (*e.g.*, human error).

The term ''subsystem'' is intended to mean, for purposes of this rule, any defined portion of a system. Subsystems will normally have distinct functions, and may constitute systems themselves.

The term ''system'' is intended to mean a composite of people, procedures and equipment which are integrated to control signals or train movement within a railroad. (Adapted from Roland, Harold E. and Moriarty, Brian, ''System Safety Engineering and Management,'' Second Edition, John Wiley and Sons, Inc., 1990, p. 6.)

The term ''system safety precedence'' is intended to capture the concept of a priority of means for hazard elimination or mitigation, as stated in Military Standard 882C, ''System Safety Program Requirements'' (U.S. Department of Defense; January 18, 1993).

The term ''validation'' is slightly modified from the IEEE definition to incorporate the notion that validation procedures do not end with the end of the development cycle. Validation can be performed at any stage of a product's life cycle, including and especially after modifications are made to it. One supplier indicated that this definition ought to be modified to exclude references to what stages in a product's life-cycle validation is performed. Comments were solicited on this issue and most commenters concurred with the definition proposed in the NPRM. The dissenting commenter stressed the need to use existing definitions thereby advocating the use of the IEEE definition of validation. The commenter favors the IEEE definition because it was developed by a professional organization comprised of experts in the field, but finds nothing inherently wrong with the definition proposed by FRA. FRA notes the commenter's concern for consistency and the use of existing definitions, but is still inclined to use the definition proposed in the NPRM. Accordingly, the definition of validation does not change.

Section 236.905 Railroad Safety Program Plan (RSPP)

The system approach to safety is used pervasively in a variety of industries to reduce the risk of accidents and injuries. FRA has discussed the need for this approach to safety in three previous rulemakings: FOX High Speed Rail Safety Standards, NPRM, 62 FR 65478, (Dec. 12, 1997); Passenger Train Emergency Preparedness, final rule, 63 FR 24630, (May 4, 1998); and Passenger Equipment Safety Standards, final rule, 64 FR 25540, (May 12, 1999). System safety means the application of design, operating, technical, and management techniques and principles throughout the life cycle of a system to reduce hazards and unsafe conditions to the lowest level possible, through the most effective use of available resources. The system safety approach requires an organization to identify and evaluate safety hazards that exist in any portion of the organization's ''system,'' including those caused by interrelationships between various subsystems or components of that system. The organization then creates a plan designed to eliminate or mitigate those hazards. Where possible, the development of a system safety plan precedes the design, implementation, and operation of the system, so that potential risks are eliminated at the earliest possible opportunity. System safety plans are viewed as living documents, which should be updated as circumstances or safety priorities change or new information becomes available.

This section requires that railroads implement FRA-approved system safety plans known as Railroad Safety Program Plans (RSPP), enforce them, and update them as necessary. In this process, the railroad is required to implement their RSPP to identify and manage safety risks, and generate data for use in making safety decisions. Based on the philosophy of system safety planning, FRA believes that initiating this process prior to design and implementation of products covered by subpart H is necessary for development of safety-critical processor-based signal and train control systems.

Paragraph (a) requires the railroad to adopt an RSPP. FRA envisions that the RSPP will be a living document that evolves as new information and knowledge become available. Due to the critical role that the RSPP plays in this final rule, FRA is requiring the railroad to submit its initial plan for FRA review and approval prior to implementation of safety-critical products. Since the development of many safety-critical features in products will be guided by the RSPP, FRA believes that its review and approval is essential. FRA feels this role is a logical and necessary outgrowth of its responsibility to promulgate clear, enforceable, and effective safety standards. This paragraph also requires the railroad to submit its initial RSPP to FRA. FRA believes that the RSPP must be used as a guide in the earliest conceptual stages of a project.

FRA received general comments addressing the system safety approach suggesting that FRA provide sample documents or templates detailing format for the RSPP, as well as other documents required by the rule. FRA has decided that providing samples or

templates would not be appropriate, since the railroad's system safety approach will likely dictate the format for any documents submitted. FRA acknowledges that based on initial drafts of the RSPPs provided by various pilot projects, the document is general in nature and lacking details regarding new systems, making the Product Safety Plan (PSP) discussed below, and review of the PSP by FRA, crucial to FRA's safety enforcement role.

Paragraph (b) requires that the RSPP address minimum requirements for development of safety-critical products. It provides minimum requirements which the RSPP must address. FRA intends the plan to be a formal step-by-step process which covers: identification of all safety requirements that govern the operation of a system; evaluation of the total system to identify known or potential safety hazards that may arise over the life cycle of the system; identification of all safety issues during the design phase of the process; elimination or reduction of the risk posed by the hazards identified; resolution of safety issues presented; development of a process to track progress; and development of a program of testing and analysis to demonstrate that safety requirements are met. These minimum requirements are addressed in paragraphs (b)(1) through (b)(4).

FRA received general comments contending that much of the information requested in paragraph (b) is information that does not typically reside with the railroad but is normally information the developer or supplier maintains. The comments further explain that railroads, as the users of various systems, are not realistically expected to know the design criteria requested in paragraph (b). Although FRA understands and appreciates the commenter's concerns, FRA has decided that railroads will remain primarily responsible for providing the requested information, as railroads have the primary responsibility for the safety of their operations. Railroads should make the necessary arrangements to ensure this information is readily available from the supplier for submission to the agency.

Paragraph (b)(1) requires that the RSPP provide a detailed description of the tasks to be completed during the preliminary hazard analysis for every safety-critical product developed for use on the railroad. Paragraphs (b)(1)(i) through (b)(1)(iv) list several types of tasks which must be included in the RSPP. Railroads have indicated that requirement (iv), the identification of the safety assessment process, appears to duplicate (ii), the complete description of risk assessment procedures. FRA intends the risk assessment to be a measurement tool, used to benchmark safety levels and hopefully to provide valuable safety insight to designers. FRA views the safety assessment process as a more comprehensive process in which safety concerns are effectively identified and addressed at all stages of product development.

FRA sought comment on the railroads' claim and FRA's distinction. FRA received several comments concluding that the two concepts were confusing, as presented. One comment proposed language to further clarify the distinction. The commenter proposed that (b)(ii) be revised to read, ''A complete description of risk assessment procedures used to benchmark safety/risk levels.'' The commenter offered a revision of (b)(iv) which would read, ''The identification of the complete safety assessment process used to identify and address all safety concerns at all stages of product development.'' FRA did not find the language particularly enhancing or clarifying and has decided not to adopt the language for the final rule. Another commenter suggested that requiring a complete description of the risk assessment procedures may actually work in opposition to the goal of using the latest evaluation techniques. The commenter recommended a summary description of the risk assessment procedure which references a complete description of either a recognized standard or detailed procedure be included in the RSPP. Although FRA understands the commenter's point, FRA has decided to allow the rule text to remain the same. FRA believes the discussion noted above has served to clarify the distinction between the risk assessment and safety assessment. Although the commenters suggested the rule text was confusing, each commenter correctly described the two concepts and their differences. FRA does not believe a rule text change is necessary or helpful here.

Paragraph (b)(2) addresses how the RSPP identifies validation and verification methods for the initial design/development process and future changes, including any standards to be complied with in the validation and verification process. The objective is that a railroad create and maintain documentation which will facilitate an independent third party assessment, if required (see § 236.915(h)). FRA believes this process will also help to refine and standardize validation and verification processes for each railroad. FRA received one comment addressing this paragraph. The commenter suggested that an internal supplier's standards and procedures related to design verification and validation be exempt from this requirement. FRA believes that the approving agency, as well as a third party reviewer may have a need to see the actual standard. FRA has decided to make a slight change in the rule text to accommodate the commenter's concern. The last sentence of paragraph (b)(2) is revised to read, ''The RSPP must require that references to any non-published standards be included in the PSP.'' This change allows FRA the flexibility to require the supplier to provide a copy of the standard if necessary.

Paragraph (b)(3) requires that the RSPP contain a description of the process used during product development to identify and consider the human-machine interfaces (HMIs) which affect safety. The requirements set forth in this paragraph and in Appendix E attempt to mandate design consideration of, among other concerns, sound ergonomic design practices for cab layout in order to minimize the risk of human error, attention loss, and operator fatigue. FRA believes it is necessary for railroads/product manufacturers to be able to demonstrate how their human factors design requirements are developed and that they are developed at an early stage in the product development process.

Paragraph (b)(4) explains how the RSPP identifies configuration management requirements for products subject to subpart H. FRA believes that this requirement is necessary to help railroads maintain consistency in the configuration management of the products they use.

Paragraph (c) describes the initial review and approval procedures FRA will utilize when considering each railroad's RSPP. Paragraph (c)(1) indicates that the petition must be delivered to the Associate Administrator for Safety, for his or her respective action. Paragraph (c)(2) establishes the timing of the petition process. FRA normally responds in some fashion within 180 days with one of the responses listed (granting the petition, denying the petition, or requesting additional information). However, there may be circumstances in which FRA is unable to respond as planned. Consequently, paragraph (c)(3) indicates that inaction by FRA within the 180-day period means the petition will remain pending. The petition is not approved until the railroad receives an affirmative grant from FRA.

FRA invited and received comments addressing FRA's handling of RSPP petitions beyond 180 days after filing.

Commenters expressed concern that FRA will delay their implementation process, by allowing petitions to remain pending. In addition, commenters view this approach as a significant departure from typical approval procedures where petitions are deemed approved, unless written notification is given to the contrary. Railroads believe the delay will impact the costs of their projects. FRA does not anticipate that petition review will typically take more than 180 days. However, in the unlikely instance that the agency is unable to process petitions within the normal period of time, the agency has allowed itself an open window to address petitions with complicated or problematic issues. FRA firmly believes that its occasional need to extend the review period for petitions will not significantly delay production or impact costs greatly and has decided against changing the approval process.

Paragraph (c)(4) provides that FRA be able to reopen consideration for any previously-approved petition for cause. This will help ensure that FRA has the ability to preempt problems erupting as a result of widely disparate safety priorities being implemented throughout the industry. Commenters who expressed concerns regarding paragraph (c)(3) also expressed concerns about paragraph (c)(4), citing similar reasons. These comments contend that the ability to reopen approved petitions for further review on the basis of unspecified criteria would only further delay implementation and in some cases may actually disrupt service. FRA disagrees with this comment as well, as this measure will be used in only rare cases. FRA has imposed a requirement upon itself to provide the railroad with specific reasons for such actions. This measure requires the agency to be able to provide clearly articulated reasons, not vague concerns for reopening the petitions. As noted with paragraph (c)(3), FRA foresees reopening petitions for cause in only the most problematic cases where any delay, cost or potential disruption in service will be balanced by FRA's responsibility to ensure safety.

Paragraph (d) establishes requirements for how and when RSPPs can be modified. First, FRA believes railroads can and should modify their RSPPs at any time. However, when RSPP modifications related to safety-critical PSP requirements are involved, FRA feels its approval is necessary. Paragraph (d)(1) requires that railroads obtain FRA approval in these cases. In any other case, the railroad would be able to implement the modification without FRA approval. Paragraph (d)(2) explains that procedures for obtaining FRA approval of RSPP modifications are the same for those used to obtain initial FRA approval, with the added requirements that the petition identify the proposed modifications, the reason for the modifications, and the effect of the modifications on safety.

Section 236.907 Product Safety Plan (PSP)

This section describes the contents of the Product Safety Plan (PSP) that must be developed to govern each product. The provisions of this section require each PSP to include all the elements and practices listed in this section to assure these products are developed consistent with generally-accepted principles and risk-oriented proof of safety methods surrounding this technology. Further, each PSP must include acceptable procedures for the implementation, testing, and maintenance of the product.

FRA's existing regulations covering signal and train control systems do not include requirements of such detail since they are based on minimum design standards of long standing application that are recognized as appropriate to achieve the expected level of performance. As a result of the industry's desire to move to ''performance-based standards'' for signal and train control systems, FRA believes it is necessary to include the provisions contained in this section in order to assure safety of railroad employees, the public, and the movement of trains. In addition, FRA must ensure that key elements in the development of products correlate with the concepts of proven standards for existing signal and train control systems.

FRA sought comments on whether the elements contained in this section are adequate or whether there are other requirements that should be included to assure safety. FRA received one comment concluding that no additional requirements were necessary to ensure safety. FRA received another comment which did not explore the PSP requirements and their relationship to safety, but looked at their relationship to cost. The commenter concluded that generally, much of the information required in this section is not currently required for processor-based systems, as they are typically designed independent of railroad operational characteristics. The comment further reasoned that requiring an analysis of the system inclusive of these operating characteristics will increase the cost of development. FRA believes that suppliers and railroads will develop generic PSPs for most products that adequately address the requirements of the new subpart without substantial additional expense. It is true that the use of general purpose processors and their associated software brings about the availability of a large number of additional features and capabilities that may or may not be used in support of the primary intended function of the designer. As part of the design and evaluation process it is essential to ensure that an adequate analysis of the features and capabilities is made to minimize the possibility that conflicts may result by the use of features resulting in a software fault. Since this analysis is a normal cost of software engineering development, we do not believe it imposes a significant cost beyond what should already be done when developing safety critical software.

Paragraph (a)(1) requires that the PSP include system specifications that describe the overall product and identify each component and its physical relationship in the system. FRA will not dictate a specific product architecture but will examine each to fully understand how various parts relate to one another within a system. Safety-critical functions in particular will be reviewed to determine whether they are designed on the fail-safe principle. FRA believes this provision is an important element that can be applied to determine whether safety is maximized and maintainability can be achieved. During early discussions, prior to publication of the NPRM, concern emerged regarding the level of detail required in describing the product. FRA requested but received no comments on this issue. Accordingly, the rule language will remain the same.

Paragraph (a)(2) requires a description of the operation where the product will be used. FRA is essentially attempting to determine the type of operation on which the product is designed to be used. One signal system supplier noted that this paragraph may not be applicable to products which are independent of some or all of the railroad operation characteristics described in this paragraph. FRA requested comment on this issue and one commenter gave an example of a product where one (or potentially several) of the operational characteristics would not apply. The example cited was an interlocking controller where gross tonnage would not be relevant. In this instance, FRA would expect a short statement indicating which operational characteristics did not apply and why they were not applicable.

Paragraph (a)(3) requires the PSP to include a concepts of operations

document containing a description of the product functional characteristics and how various components within the system are controlled. FRA believes that this provision along with that contained in paragraph (a)(1) above will assist in a thorough understanding of the product. FRA will use this information to review the product for completeness of design for safety by comparing the functionalities with those contained in standards for existing signal and train control systems. While FRA will not prescribe standards for product design, FRA will require that the applicant compare the concepts contained in existing standards to the operational concepts, functionalities, and control contemplated for the product. For example, FRA requirements prescribe that where a track relay is de-energized, a switch or derail is improperly lined, a rail is removed, or a control circuit is opened, each signal governing movements into a block occupied by a train, locomotive, or car must display its most restrictive aspect for the safety of train operations. FRA intends to apply the same concept, among others, when reviewing PSPs to assure such minimum safety requirements exist.

Paragraph (a)(4) requires that the PSP include a safety requirements document that identifies and describes each safety-critical function of the product. FRA intends to use this information to determine that appropriate safety concepts have been incorporated into the proposed product. For example, existing regulations require that when a route has been cleared for a train movement it cannot be changed until the governing signal has been caused to display its most restrictive indication and a predetermined time interval has expired where time locking is used or where a train is in approach to the location where approach locking is used. FRA will apply this concept, among others, to determine whether all the safety-critical functions are included. Where such functionalities are not clearly determined to exist as a result of technology development, FRA will expect the reasoning to be stated and a justification provided describing how that technology provides equivalent or greater safety. Where FRA identifies a void in safety-critical functions, FRA will expect remedial action prior to use of the system. FRA received no comments specifically addressing the adequacy of this process for preserving railroad safety and has not changed the rule text.

Paragraph (a)(5) requires the PSP to contain a document demonstrating that the product architecture satisfies the safety requirements. The product architecture is expected to cover both hardware and software aspects which identify the protection developed against random hardware faults and systematic errors. Further, the document should identify the extent to which the architecture is fault tolerant. This provision may be included in the requirements of paragraph (a)(1).

Paragraph (a)(6) requires that a hazard log be included in the PSP. This log consists of a comprehensive description of all hazards to be addressed during the life-cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence). The hazard log addresses safety-relevant hazards, or incidents/failures which affect the safety and risk assumptions of the product. Safety-relevant hazards include events such as false proceed signal indications and false restrictive signal indications. If false restrictive signal indications happen with any type of frequency, they could cause train crew members or other users (roadway workers, dispatchers, etc.) to develop a lackadaisical attitude towards complying with signal indications or instructions from the product, creating human factors problems. Incidents in which stop indications are inappropriately displayed may also necessitate sudden brake applications that may involve risk of derailment due to in-train forces. Other unsafe or wrong-side failures which affect the safety of the product will be recorded on the hazard log. The intent of this paragraph is to identify all possible safety-relevant hazards which would have a negative effect on the safety of the product. Right-side failures, or product failures which have no adverse effect on the safety of the product (*i.e.*, do not result in a hazard) would not be required to be recorded on the hazard log.

FRA received a comment suggesting that FRA's reference to threshold limits in the hazard log is essentially the same as quantitative risk assessment. This commenter recommended use of the MIIL–STD–882 classifications. This issue was addressed in discussions at the San Antonio meeting of the Working Group. Opposition to the use of the MIL–STD–882 was articulated, as well as concern that the comment was not really applicable to the section. FRA has decided that the MIL–STD–882 is not appropriate here and accordingly, the text will remain the same.

Paragraph (a)(7) requires that a risk assessment be included in the PSP. FRA will use this information as a basis to confirm compliance with the minimum performance standard.

Paragraph (a)(8) requires that a hazard mitigation analysis be included in the PSP. The hazard mitigation analysis must identify the techniques used to investigate the consequences of various hazards and list all hazards addressed in the system hardware and software including failure mode, possible cause, effect of failure, and remedial actions. A safety-critical system must satisfy certain specific safety requirements. Leveson, Nancy G., ''Safeware: System Safety and Computers,'' Addison-Wesley Publishing Company, 1995. To determine if these requirements are satisfied, the safety assessor must review and assess the results of the following tasks:

1. Hazards associated with the system have been comprehensively identified.
2. Hazards have been appropriately categorized according to risk (likelihood and severity).
3. Appropriate techniques for mitigating the hazards have been identified.
4. Hazard mitigation techniques have been effectively applied.

FRA does not expect that the safety assessment will prove that a product is absolutely safe. However, the safety assessment should provide evidence that risks associated with the product have been carefully considered and that steps have been taken to eliminate or mitigate them. Hazards associated with product use need to be identified, with particular focus on those hazards found to have significant safety effects. Then, the designer must take steps to remove them or mitigate their effects. Hazard analysis methods are employed to identify, eliminate and mitigate hazards. Under certain circumstances, these methods will be required to be reviewed by an independent third party for FRA approval.

FRA received a general comment indicating that the requirements of paragraphs (a)(6) and (a)(8) should be combined and required as one document. The concern presented here is similar to one echoed in several comments regarding the format for both the RSPP and PSP. Some comments requested sample documents to be used as templates by the railroads. FRA is not dictating the format in which the information should be submitted, as the variation in railroad and product will likely drive the outcome of the document. However, FRA believes that documents submitted for the North American Joint PTC Illinois project can be looked to as examples, but are not intended to be a template for submissions. FRA believes the issue of combining the requirements of

paragraphs (a)(6) and (a)(8) into one document is one of format and should be resolved by the submitting railroad. Submissions for the Illinois project can be consulted for examples.

Paragraph (a)(9) also requires that the PSP address safety verification and validation procedures. FRA believes verification and validation for safety are vital parts of the development of products. Verification and validation requires forward planning and, consequently, the PSP should identify the test planning at each stage of development and the levels of rigor applied during the testing process. FRA will use this information to assure the adequacy and coverage of the tests are appropriate.

Paragraph (a)(10) requires the PSP to include the results of the safety assessment process by analysis that identifies each potential hazard and an evaluation of the events leading to the hazard; identification of safety-critical subsystems; the safety integrity level of each safety-critical subsystem; design of each safety-critical subsystem; results of a safety integrity analysis to assess the safety integrity level achieved by the safety-critical subsystems; and ensure from the analysis that the safety integrity levels have been achieved. FRA expects the safety assessment process to be clearly stated and thorough according to the complexity of the product. FRA realizes that paragraphs (a)(9) and (a)(10) may overlap in terms of requirements, and considered consolidation of the concepts required in these two paragraphs. FRA decided to leave the rule language unchanged. The agency has an expectation of some repetition in the railroad's submissions.

Paragraph (a)(11) requires a human factors analysis which addresses all human-machine interfaces (HMI's) and all product functions to be performed by humans to enhance or preserve safety. FRA expects this analysis to place special emphasis on human factors coverage of safety-critical hazards including the consequences of human failure to perform. Each HMI is to be addressed including the basis of assumptions used for selecting each such interface, its effect upon safety and identification of potential hazards associated with each interface. Where more than one employee is expected to perform duties dependent upon the output of, or input to, the HMI, the analysis must address the consequences of human failure to perform singly or in multiple. FRA uses this information to determine the HMI's effect upon the safety of railroad operations. The human factors analysis must address all criteria listed in Appendix E, unless approval is obtained from the Associate Administrator for Safety to use other equally suitable criteria. FRA believes that designers must have this flexibility.

Paragraph (a)(12) requires the railroad to include in its PSP the training, qualification, and designation program for workers whether or not railroad employees who will perform inspection, testing, and maintenance tasks involving the product. FRA believes many benefits accrue from the investment in comprehensive training programs which, among other things, are fundamental to creating a safe workforce. Effective training programs can result in fewer instances of human casualties and defective equipment, leading to increased operating efficiencies, less troubleshooting, and decreased costs. FRA expects any training program to include employees, supervisors and contractors engaged in railroad operations, installation, repair, modification, testing, or maintenance of equipment and structures associated with the product.

Paragraph (a)(13) requires the PSP to identify specific procedures and test equipment necessary to ensure the safe operation, installation, repair, modification and testing of the product. Requirements for operation of the system must be succinct in every respect. The procedures must be specific about the methodology to be employed for each test to be performed that is required for installation, repair, or modification including documenting the results thereof. FRA will review and compare the repair and test procedures for adequacy against existing similar requirements prescribed for signal and train control systems. FRA will use this information to ascertain whether the product will be properly installed, maintained, and tested.

Paragraph (a)(14) provides that products may be so designed that existing requirements contained in part 236, subparts A, B, C, D, E, and F are not applicable. In this event, the PSP must identify each pertinent requirement considered to be inapplicable, fully describe the alternative method used that equates to that requirement and explain how the alternative method fulfills or exceeds the provisions of the requirement. FRA notes that certain sections of part 236 may always be applicable to subpart H products. For example, § 236.0 prescribes, among other requirements, the conditions and speeds for which block signal systems and automatic cab signal, train stop, and train control systems must be installed. These are benchmark safety levels related to operational considerations against which the safety performance of innovative newer systems will be compared. Further, FRA will determine whether the product fully embodies the concepts of proven standards for existing signal and train control systems, as captured by subparts A–G of part 236.

Paragraph (a)(15) requires the PSP to include a description of the security measures necessary to meet the specifications for each product. Security is an important element in the design and development of products and covers issues such as developing measures to prevent hackers from gaining access to software and developing measures to preclude sudden system shutdown. The description should identify the formal method used in development of the system software, identify each hazard and its consequence in event of failure that was mitigated by using the formal method, and indicate the results of the formal proofs of correctness of the design. Where two or more subsystems or components within a system have differing specifications, the description should address the safety measures for each subsystem or component and how the correctness of the relationships between the different specifications was verified. Where two formal methods are used in developing safety-critical software from the same specification, the description should explain why the more rigorous method was not used throughout development process and the effect on the design and implementation.

FRA received several comments on paragraph (a)(15), including one that suggested refining the concept of ''security measures.'' FRA is reluctant to modify the text or refine the concept, as FRA is concerned about all dimensions of security.

Paragraph (a)(16) requires warnings to ensure safety is addressed in the Operations and Maintenance Manual and warning labels placed on the equipment of each product as necessary. Such warnings include, but are not limited to, means to prevent unauthorized access to the system; warnings of electrical shock hazards; cautionary notices about improper usage, testing or operation; and configuration management of memory and databases. The PSP should provide an explanation justifying each such warning and an explanation of why there are no alternatives that would mitigate or eliminate the hazard for which the warning is placed.

Paragraph (a)(17) requires the railroad to develop comprehensive plans and

procedures for product implementation. Implementation (validation or cutover) procedures must be prepared in detail and identify the processes necessary to verify the product is properly installed and documented, including measures to provide for the safety of train operations during installation. FRA will use this information to ascertain the product will be properly installed, maintained, and tested.

Paragraph (a)(18)(i) requires the railroad to provide a complete description of the particulars concerning measures required to assure products, once implemented, continue to provide the expected safety level without degradation or variation over their life cycles. The measures must be specific regarding prescribed intervals and criteria for testing; scheduled preventive maintenance requirements; procedures for configuration management; and procedures for modifications, repair, replacement and adjustment of equipment. FRA intends to use this information, among other data, to monitor the product to assure it continues to function as intended.

Paragraph (a)(18)(ii) provides a PSP requirement to include a description of each record concerning safe operation. Recordkeeping requirements for each product are discussed in § 236.917.

Paragraph (a)(19) requires that the PSP include a description of all backup methods of operation and safety critical assumptions regarding availability of the product. FRA believes this information is essential for making determinations about the safety of a product and both the immediate and long-term effect of its failure. Railroads have indicated concern that product availability is not in itself a safety function, and that therefore this requirement may be too broad. FRA has contended that availability is directly related to safety to the extent the backup means of controlling operations involves greater risk (either inherently or because it is infrequently practiced). FRA invited comment on this issue but received none.

Paragraph (a)(20) requires that the PSP include a complete description of all incremental and predefined changes.

Paragraph (b) addresses predefined changes. PSPs must identify the various configurable applications of the product, since this rule mandates use of the product only in the manner described in its PSP (see § 236.915(d)). FRA recognizes that railroads' rights-of-way vary with regard to the number of tracks and layouts of interlockings, junctions and stations over which train movements are made at various speeds and density. Products may contain identical subsystems or components having configurable features to provide the capability of controlling a variety of track layout schemes. The PSP must clearly set forth those attributes in such equipment that may be employed or expunged without degradation or variation of safety over the life cycle of the system, as well as the impact such changes may have in the risk assessment. Satisfaction of the minimum performance standard must be demonstrated for each predefined change. Also, the PSP must fully describe the procedures to be followed for each change and the inspections and tests necessary to assure the system functions as intended.

Paragraph (c) addresses incremental and maintenance changes and changes classified as safety-critical software upgrades, patches, or revisions. The term ''incremental change'' is intended to capture the concept of planned version changes to a product, usually software-type changes. FRA believes these changes will be necessary in order for products to acquire capabilities to perform added functions as safety requirements change. The goal of this paragraph is to encourage as many subsequent product modifications as possible to be considered by initial designers during the product development stage, in order to avoid, to the extent possible, changes made by persons with no link to initial safety design considerations.

The NPRM recognized that hardware and software suppliers were in the best position to know about problems with the products used by the railroads. Commenters indicated that much of the information generally needed for compliance with this rule typically resides with the supplier. Suppliers will likely have information regarding problems with their products. Given the importance of proper configuration management in safety critical systems, FRA believes it is essential that railroads learn of and take appropriate action to address all safety critical software upgrades, patches or revisions for their processor-based system, subsystem, or component, whether or not the railroads have experienced a failure of their system, subsystem, or component. At the same time, FRA recognizes the complexity of the electronics market. Some software will be provided by non-railroad suppliers, often embedded in hardware. Other software may be imported from non-railroad applications; and neither the railroad nor the system integrator (supplier to the railroad) may have access to all information regarding coding errors or hardware failures. Business failures will occur, and competent supply houses may lose their technical edge over time.

FRA seeks to encourage commercial relationships that will contribute to product support over the long term; however, what is perhaps more critical to FRA's oversight role is obtaining a clear understanding of the robustness of the information network available to the railroad for life cycle product maintenance and thus of the residual risk associated with any gaps in that network.

Accordingly, FRA is responding to such comments in the area of configuration management by adding text to the rule requiring railroads disclose arrangements with their suppliers for product support, which would typically include immediate notification of all safety critical software upgrades, patches, or revisions for their processor-based system, subsystem, or component. FRA will be looking for evidence of this arrangement between railroad and supplier in its review in accordance with § 236.909(b). Failure to have such an agreement with a supplier will likely impact FRA's determination with a high degree of confidence that introduction of the new system will not result in a degradation of safety.

Upon such notification and provision of software changes, the upgrade, patch, or revision must be installed without undue delay. Until the software upgrade, patch, or revision has been installed, a railroad must treat the product as if a safety critical hazard exists and take the appropriate action specified in the PSP and by the supplier. FRA believes this is necessary to ensure that any component changes that, if left uncorrected would increase risk or interfere with the safety of train operations, are promptly addressed and that a common safety baseline is maintained.

In particular, FRA believes it is the responsibility of the railroads to either develop a mutually acceptable external contractual relationship with software developers capable of providing the required timely software support or to demonstrate they have in-house software development capability to provide the necessary support . FRA would expect that this support would include providing the necessary safety software upgrade, patch or revisions after determination of a need, identification of the specific product and software version involved, the nature of the risk, any recommended mitigation pending assurance of the corrected software, and any necessary regression testing. Lack of such a fundamental life cycle software support

capability would call into question the long term suitability of the software for safety critical operations. Similar concerns apply to specialized hardware.

The final rule requires railroads to disclose these relationships. FRA intends to look for these relationships in its PSP reviews. FRA will intervene in accordance with § 236.913(g)(5) by reopening consideration of a PSP petition for cause, if there is a breakdown in communications that could adversely affect public safety. FRA will attempt to facilitate communications between the parties involved prior to formally reopening review. In the event that the need for a modification to safety critical software is identified, and the product developer is no longer in business or is unwilling to support the product, FRA will work with the affected railroads and supplier trade organizations in determining an appropriate course of action taking into consideration the extent and severity of the situation, and the availability of the original source code.

Since not all railroads may experience the same software faults or hardware failures, the developer's software development, configuration management, and fault reporting tracking system play a crucial role in the ability of the railroad and the FRA to be able to determine and fully understand the risks and their implications. Without an effective configuration management tracking system in place it is difficult, if not impossible, to fairly evaluate risks associated with a product over the life of the product. FRA expects railroads to enter into contractual arrangements with the software suppliers to ensure that the railroad is made aware of problems occurring with the software they use.

The new language also places a direct obligation on suppliers to report safety-relevant failures, which would include ''wrong-side'' failures and failures significantly impacting on availability where the PSP indicates availability to be a material issue in the safety performance of the larger railroad system. Suppliers would take on this responsibility under contract to the railroad (as disclosed in the PSP). The provision is necessary to ensure public safety in any case where a commercial dispute (*e.g.*, over liability) might disrupt communication between a railroad and supplier.

Section 236.909 Minimum Performance Standard

FRA is issuing a substantive standard which is performance-based rather than prescriptive. In short, FRA desires to establish what level of performance must be achieved, but not how it must be achieved. The objective of the minimum performance standard FRA requires is simple: new processor-based signal and train control systems must be at least as safe as the systems they would replace. The challenge inherent in this performance-based standard is measuring performance levels. For FRA, this challenge becomes one of being able to confirm compliance.

Paragraph (a) establishes the performance standard for all products to be covered by this rule. The railroad must establish with a high degree of confidence through its safety analysis that introduction of the system will not result in a safety risk level that exceeds the level of safety risk in the previous condition. In short, the railroad must prove that safety is not degraded. This standard places the burden on the railroad to demonstrate that the safety analysis provides a high degree of confidence. Under this regulatory scheme, FRA will have access to the railroads' analyses, and will be likely to detect obvious shortcomings in them.

Paragraph (b) indicates that the FRA Associate Administrator for Safety will rely on the factors listed in § 236.913(g)(2) when assessing whether the petitioner has met the performance standard for the product through employment of sufficient safety analysis. ''FRA review of PSP'' is intended to apply to both FRA review of petitions for approval and FRA review of informational filings, which, for good cause, are treated as petitions for approval. Railroads have indicated concern that this proposal does not provide for an administrative appeals procedure. FRA believes that final agency determinations under this subpart should be made at the technical level, rather than the policy level, due to the complex and sometimes esoteric subject matter. FRA sought comment on the concern and its view and received one comment in agreement with the agency view of an administrative appeals process. FRA has not changed the rule text.

Paragraphs (c) and (d) establish standards for the scope of the risk assessment to be conducted. Unless criteria for an abbreviated risk assessment are met, a full risk assessment would be required for each product.

Paragraph (c) describes the scope for a full risk assessment. The risk assessment need only address risks relevant to safety of the product. For instance, the risk of injury due to a broken handhold on a freight car would not be affected by implementation of a new signal and train control system, and therefore need not be included in the risk assessment. However, any risk which is affected by introduction, modification, replacement or enhancement of the product must be accounted for. The standard further explains that these risks can be broken down into three categories to include: New risks, eliminated risks, and risks neither new nor eliminated whose nature (probability of occurrence or severity) has changed. FRA understands that many of the affected risks relate to very low probability events with severe consequences. These risks might be overwhelmed if analyzed in combination with other, more probable risks, which would not be affected by the change.

Paragraph (d) establishes a simpler approach to demonstrate compliance with the performance standard for less complex changes such as replacement of certain signal and train control system components. FRA is allowing this simpler approach when the type of change is sufficiently basic. This proposed class of changes is defined as one which does not introduce any new hazards into the railroad operation (that is, different from the previous method of operation) and which maintains the same (or lower) levels of risk exposure and severity for hazards associated with the previous condition. FRA felt comfortable with this distinction since no new hazards are introduced with introduction of the product, and hazards which were present in the original operation are sufficiently contained (not increased in severity or exposure thereto). An example of this type of change would be replacement of a component in a signal and train control system with a newer-generation processor-based component which performs the same function. No new hazards would likely be introduced that weren't already there, original hazards would not be subject to higher exposure, and original hazards would not be subject to an increase in severity. Unless introduction of the new product is accompanied by changes in operation, the hazards encountered by the new product (which will normally be a component of the system) would be identical in both severity and exposure.

FRA received a comment indicating that the text as drafted in the NPRM did not clearly express the concept. The proposed text stated,

> An abbreviated risk assessment demonstrates that the resulting MTTHE for the proposed product is greater than the MTTHE for the product or methods performing the same function in the previous condition.

FRA agrees with the commenter and is modifying the text to state,

> An abbreviated risk assessment supports the finding required by paragraph (a) of this section if it establishes that the resulting MTTHE for the proposed product is greater than or equal to the MTTHE for the system component or method performing the same function in the previous condition.

For changes analyzed using this simplified analysis, risk associated with operation under the new product is assumed to be proportional to its MTTHE. Therefore, changes in risk are assumed to be proportional to changes in MTTHE. This simplified approach was based on the principle that when risk severity and risk exposure remain constant, risk is directly proportional to the probability of a hazardous event occurring. This is demonstrated by the equation: $risk_h = probability_h * severity_h$. which in basic terms, states that the risk of a hazard occurring is equal to the probability of the hazard occurring multiplied by the severity of the hazard. The product's MTTHE is a convenient indication of hazard probability levels for two reasons. First, suppliers have indicated that MTTHE figures can be made readily available since they are already used by some railroad signal and train control system suppliers of off-the-shelf components used in those systems. Second, MTTHE is inversely related to the hazard probability identified in the equation above.

If in the above equation the hazard severity is kept constant, hazard probability remains directly proportional to the risk. This is true only if the exposure to the risk, which is related primarily to railroad operating practices (*i.e.*, train speeds, train volumes, utilization of product, etc.), remains the same. This way risk associated with operation under the resulting system is directly proportional to the MTTHE of the new product. This condition on risk exposure is necessary since it precludes changes in train volume or other operating practices which may affect the actual safety risk encountered.

During early Working Group discussions, prior to publication of the NPRM, suppliers requested that severity not be locked into place in order to fit into this exception, but also to allow for cases where introduction of the product may bring about a reduction in hazard severity. Although an example might be difficult to imagine, FRA is confident that in such case it is mathematically impossible for safety risk levels to increase. Under these conditions, the FRA feels that MTTHE is a sufficient indication of risk, thereby warranting a simplified risk assessment. If a more complex risk assessment is more advantageous to the supplier or railroad, the rule permits that approach.

FRA invited comments on whether this exception from the full rigors of the risk assessment is appropriate, and if not, to what extent the required analysis should become more rigorous as the complexity of the proposed system increases. FRA received one comment asking for guidance regarding the level of proof necessary to fall into this exception. Despite informative discussion on this comment, FRA could not develop language that would further clarify this point. FRA has further reviewed the language and found the requirements of paragraph (d) have sufficient detail to provide the necessary guidance. FRA has no interest in preventing use of the abbreviated risk assessment, when appropriate.

FRA has reviewed paragraph (d) in an effort to create some additional flexibility and to improve clarity. The paragraph has been revised from the NPRM to place the explanation of when an abbreviated risk assessment may be used, at the beginning. In addition, FRA also endeavored to respond to a comment from the supplier community seeking an opportunity to utilize traditional methods as an alternative approach for analysis. To address this need, a new paragraph (d)(3) has been added that permits satisfaction of the performance standard by reference to safety criteria stated in a specified industry standard recently adopted by the American Railway Engineering and Maintenance Association (AREMA). That criterion is stated in Part 17.3.5 of the AREMA Communications & Signaling Manual (AREMA Manual) and involves the application of safety principles and procedures in the design of railway signal equipment. This alternative test also requires compliance with the principles set forth in Appendix C and with two additional named AREMA standards, AREMA Manual Part 17.3.1 and AREMA Manual Part 17.3.3. These new product development standards specify a Safety Assurance Program for Electronic/Software Based Products, Practices for Hardware Analysis, and Procedures for Hazard Identification and Management. Recognition of compliance with these standards, in conjunction with the design principles set forth in Appendix C, extends the advantages of a performance-based standard to traditional signal or train control products. In the final rule, FRA incorporates the AREMA standard by reference.

The basis for this alternative standard was suggested by railroad signal suppliers, during the final Working Group discussions on recommendations for a final rule, as a means of satisfying concerns expressed in the public comments regarding the need to hold down costs of safety analysis for traditional products built on fail safe principles. Suppliers noted that great confusion and delay could result under the proposed rule should a traditional signal or train control product be offered as a replacement for a similar product. In such a case, inconsistent supplier approaches to making estimates of unsafe failures could unnecessarily complicate safety analysis. FRA agrees that introduction of new products should not be complicated by paper exercises over small differences in theoretical risk when both the new product and the product to be replaced have been engineered to strictly limit the possibility of unsafe failures.

FRA has added new language calling for adherence to safety principles set forth in Appendix C and the new AREMA standard and permits qualification of a product even if it is not possible to achieve a high degree of confidence on the evidence that the MTTHE of the proposed product is equal to or greater than the product it is replacing. Such a case could arise in a variety of circumstances. For instance, it might prove extremely difficult to establish comparability for the new product under subpart H where replacing a similar product developed under the previous rule. In another case, the safety analysis methods of two different suppliers might not permit direct comparison of the degree to which MTTHE estimates are well founded, or the very high mean time estimates of both suppliers might render largely academic any differences. Paragraph (d) provides a solution to these conundrums.

FRA also notes there are times when differences in theoretical risk, while ''large'', are of such a nature as to have no practical effect upon the situation. In many cases, changes to these risk value can be done with little impact, because the failure in question is so unlikely to occur within the life of the product. Paragraph (d)(3) is intended to provide flexibility where there is no reason to believe that differences in MTTHE estimates reflect the potential for an actual degradation of safety.

Paragraph (e) establishes general principles for the conduct of risk assessments and which methods may be used. Paragraph (e)(2) contains general criteria for each risk calculation. FRA has identified three variables which must be provided with risk calculations: accident frequency, severity, and

exposure. Traditionally, risk is defined as the expected frequency of unsafe events multiplied by the expected consequences. FRA feels that exposure should be identified because increases in risk due to increased exposure could be easily distinguished from increases in risk due solely to implementation and use of the proposed product. FRA is primarily interested in risks relevant to use of the proposed product. FRA feels it would be inconsistent policy to insist to a railroad which intends to double its traffic on one rail line that it halve its accident rate if it puts in a new signal or train control system. Conversely, FRA feels a railroad should not be allowed to implement a new signal or train control system which projects double the original accident rate on a line simply because it intends to reduce its traffic volume on that line by one half. A requirement to identify exposure will help define risks relevant to use of the proposed product.

Risk exposure may be indicated by the total number of train miles traveled per year or total passenger miles traveled per year, if passenger operations are involved. FRA believes risk to operations involving passengers is highly relevant, since advanced train control technology will most certainly find uses on such lines. NTSB has specifically recommended application of advanced train control technology to lines with passenger traffic. NTSB/Railroad Accident Report-93/01. FRA believes any change should not adversely affect the safety of passenger operations. However, a risk assessment method which does not account separately for passenger miles could, in theory, obscure an increase in risk for passengers that was offset by a reduction in freight-related damages.

In early drafts of the NPRM, FRA had proposed to the Standards Task Force that risk measurements be adjusted for exposure in units of train-miles per year, passenger-miles per year or ton-miles per year, but that the units not be mandated in the rule. Most freight railroads keep safety data in terms of train-miles, employee hours, and in some cases gross ton-miles. Since train-mile data must be reported to FRA under part 225, FRA does not believe railroads will burden themselves additionally by maintaining other data for purposes of this requirement. Passenger-miles should be readily available from entities providing the service.

The FRA sought comment on the NPRM's proposed requirement to account for exposure in the units mentioned above, specifically regarding the appropriateness of this approach and other possible approaches. FRA received comments from suppliers indicating that railroads should have more flexibility in determining what risk parameter is appropriate. The comments indicated the use of train-miles or hours should be acceptable and the use of the MIL-STD–882 should be acceptable for severity. Discussions of this comment within the Working Group left FRA satisfied that railroads who will be required to comply with this rule will be comfortable with train-miles or passenger-miles. FRA has decided to modify the risk exposure metric for passenger operations to use passenger-miles as a measure of exposure in passenger operations, but will otherwise leave the NPRM language unchanged.

Paragraph (e)(2) also covers a requirement for risk severity measurements. FRA is allowing railroads to measure risk severity either in terms of total accident costs, including property damage, injuries and fatalities, or in simpler terms of expected fatalities only. FRA allows the two alternatives in order to allow flexibility, and to permit the railroads to avoid metrics which could be misconstrued as trading dollars for lives, when in fact they would be more comprehensive in avoiding accident consequences.

FRA wishes to make clear that the sole purpose of the risk assessment in this rule is to require railroads to produce certain safety risk data which will allow the agency to make informed decisions concerning projected safety costs and benefits. FRA feels this is a necessary component of the performance standard in order for FRA to be able to effectively carry out its statutory duties as a regulatory agency. By establishing a requirement for a risk assessment, FRA does not intend to create a presumptive amount of damages for tort liability after an accident occurs. In order to help maintain the safety focus of this requirement, FRA is allowing railroads to use only predicted fatalities as the risk metric (except in the case where passenger service is provided). FRA believes that for the types of safety risks involving signal and train control, total accident costs and total fatalities correspond closely enough to allow an accurate view. Thus FRA believes that allowing the alternative measure would not change substantially the risk assessment.

Paragraph (e)(3) involves the issue of concurrent changes in railroad operations. Railroads intending to implement products covered by subpart H may intend to change operational characteristics at the same time to take advantage of the benefits of the new technology. FRA envisions increased train volumes, passenger volumes, or operating speeds, or all three, to be likely changes to accompany implementation of subpart H products. The rule requires the railroad to analyze the total change in risk, then separately identify and distinguish risk changes associated with the use of the product itself from risk changes due to changes in operating practices (*i.e.*, risk changes due to increased/decreased operating speed, etc.). FRA believes this procedure is necessary to make an accurate comparison of the relevant risks for purposes of determining compliance with the minimum performance standard in § 236.909(a).

The second sentence of paragraph (e)(3) concerns changes in operating speeds related to required signal and train control systems for passenger and freight traffic. In such case, the provisions of § 236.0 normally apply, mandating the use of certain technologies/operating methods. Thus, for changes to operating speeds, the previous condition calculation must be made according to the assumption that such systems required by § 236.0(c) (and § 236.0(d), if applicable) are in use. This requirement ensures that a minimum level of safety set by § 236.0, which otherwise normally applies, is respected and not circumvented.

In addition to including an adjustment in the previous condition to account for increases in train speeds as addressed in § 236.0, FRA also intends that even where § 236.0 would not require upgraded systems due to speed increases, an adjustment be made if necessary to take into consideration the need for fluid traffic management. For instance, if the railroad proposed to implement a non-vital overlay train control system in dark territory in connection with major projected increases in traffic, the previous condition would need to be adjusted to assume installation of a traffic control system (which, under the options available under current part 236, would be needed as a practical matter to move the increased numbers of train across the territory). This provision was offered in the proposed rule as a result of FRA's view that operations in dark territory have a much higher risk of collision than in signal territory (when normalized on a train mile basis); accordingly, it was believed that this adjustment willset the safety baseline at an appropriate level for purpose of making the necessary comparison. FRA reasoned that failure to make this adjustment within the previous

condition would at least theoretically permit a progressive worsening of the safety situation as new technology is brought on line.

During discussions at the December 2001 Working Group meeting, the concern emerged that a density-linked trigger for adjustment of the base case could inappropriately constrain the ability of railroads to manage traffic flows across their systems and respond to shipper requirements. Questions were raised concerning the empirical basis for FRA's assumption. After independent consideration of the informative discussion, FRA agreed that the issue deserved more detailed consideration.

A small team of stakeholder representatives formed by the RSAC PTC Working Group discussed the issue of adjusting the base case, working from data on the Volpe Center's rail network. Refinements to the traffic flows were required to achieve the necessary fidelity to actual conditions during the study period.

Concern was initially expressed that risk did not go up with train frequency, that instead it appears to go down, so there was not good reason to adjust the base case. FRA maintained that risk increased with train frequency. FRA also maintained that cumulative risk on a line segment was relevant to safety, and that with current technologies railroads could not move increased train densities on most lines without installing systems such as traffic control, which greatly reduce risk. As the traffic density increases the per train-mile cost of providing traffic control systems decreases. Initial discussions promoted the conclusion by some that risk did not vary by method of operation. FRA and other stakeholders agreed that for any system, the risk would tend to increase with train speed. FRA researched the issue, through the Volpe Center and other contractors. FRA presented the research to the team, which agreed on the following:

- Risk per train mile in dark territory (*i.e.* lines with no signal or train control system) is approximately 2 times the risk of other territories, Traffic Control System (TCS), Automatic Block System (ABS), and Auto.[1]
- Risk doesn't change much with increased speed or frequency in operations already using TCS, ABS and Auto.
- Risk in dark territory does increase with speed and/or frequency.
- The cost per mile of risk from positive train control preventable accidents is about 12 cents per train-mile in dark territory and is about 6 cents per train-mile elsewhere.

These facts were based only on analysis of freight operations and excluded any passenger trains or accidents from risk metrics.

(In addition, FRA notes that within dark territory risk from positive train control preventable accidents per train-mile ranges from about 9 cents per train-mile at low density, to between 15 and 18 cents per train-mile at high density.)

FRA also presented evidence that operations with more than 12 trains per day in dark territory were rare, operations with more than 16 trains per day in dark territory were extremely rare, and operations with more than 20 trains per day in dark territory were almost nonexistent. FRA believes that high volume operations in dark territory are rare because such operations are uneconomical under current regulations. FRA believes that a functioning market induces railroads to adopt signal systems, which promote safety and fluid train movement in higher volume operations, for purely business reasons, but that if the rule here were to go into effect without adjusted base case provisions, then some railroads might adopt systems which were not as safe as TCS in high volume operations, creating a market failure.[2]

Under the final rule as adopted, if the change in railroad operation were to result in crossing one of the speed thresholds in § 236.0, then the adjusted base case will be the system currently utilized under normal practice for that maximum authorized speed. For freight speeds exceeding 49 miles per hour and passenger speeds exceeding 59 miles per hour, the base case will be a traffic control system.[3]

Where speeds exceed 79 miles per hour, § 236.0 currently requires automatic cab signals, automatic train stop, or automatic train control. However, FRA has supplemented these requirements to address specific needs as previously discussed; and essentially all planning for such investments is conducted in support of high speed passenger rail service. Intermittent automatic train stop technologies are not fail safe in nature, do not function in the event of inappropriate operator acknowledgment, and do not address overspeed operation. By itself, automatic cab signaling provides only warning of signal downgrades requiring acknowledgment without enforcement; and this configuration has been determined to be inappropriate for service on the Northeast Corridor as a result of major catastrophic events. Continuous automatic train stop paired with cab signals does not provide speed control, presenting the possibility of ineffectual intervention (and at a cost for a new installation comparable to automatic train control, which does regulate speed consistent with cab signal indications). Accordingly, FRA has scaled the triggers to reflect acceptable contemporary practice. For speeds in the range of 80 to 110 miles per hour, automatic cab signals and train control will be employed for the adjusted base case.

For speeds above 110 miles per hour, FRA will determine the appropriate base case in light of the characteristics of the planned operation and service experience within the speed range. Factors that will be considered include average train speeds, mix of traffic, complexity of the operation, presence or absence of special hazards (*e.g.*, movable bridges, extreme curvature), intended curving speeds and associated cant deficiencies. In this speed range, provisions for safety must be particularly rigorous because of the highly catastrophic consequences that can occur in the case of a mishap. Application of professional judgment is necessary to discern practical responses to known hazards in such environments, and through this approach the difficulty of estimating the frequency of very rare events can be reduced (in effect closing the gap

[1] Auto was a construct which included high-performance signal systems, including automatic train stop and cab signals.

[2] We refer to a market failure when the normal functioning of the economic system does not adequately address safety without the necessity of intervention through regulation. For instance, in an environment where investments in on-board train control technology are uneven, and railroads share locomotives, no railroad may have an incentive from a safety point of view to go forward with a highly effective train control installation. Failing effective cooperation among railroads, which has thus far not materialized (even though such systems have now been under discussion for almost 20 years), railroads may be driven toward low-cost options that do not achieve a high level of safety. This can be contrasted with installation of a traffic control system, for which most of the benefits will flow to the owning railroad (but which is expensive to install on a per-mile basis).

[3] Under § 236.0, a manual block system may be used in lieu of an automatic block signal system or traffic control system; but this allowance does not reflect current safety practice and is not acceptable for further application beyond existing territory due to the absence of track circuits for broken rail detection and because of the potential for unchecked mis-communication. Current safety data indicates that an automatic block signal system supplementing verbal issuance of mandatory directives is at least as safe as traffic control, so removing that option will not disadvantage applicants; further, use of traffic control signaling is notably superior from a business point of view, as evidenced by its selection for virtually all recent signalization projects on major lines.

between differences in the base case and the new system).

As further clarification of the concept included in § 236.909(e)(3) of the NPRM, the final rule provides that the adjusted previous condition (base case) must include TCS if any change results in a volume of more than twelve trains per day, unless a specific exception applies, or an increase of more than four passenger trains per day. Volume is computed based on annual average density, so density on any given day may be considerably higher. (Accordingly, the practical implications of these density triggers for adjustment of the base case are expected to be quite limited.) FRA included a new provision which permits the railroad to demonstrate in situations where volumes will exceed 12 trains per day, but will not exceed 20, that the current method of operation is adequate for the specified volume and will not delay movement of trains nor will it unreasonably increase expenditures to expedite movement.

Questions regarding generalizing models surfaced during discussions of the risk assessment. FRA believes it is permissible to generalize a model. In reviewing a model which has been generalized, FRA will consider whether the railroad has analyzed the system where the comparison is likely to be the least favorable (*e.g.*, the new system as an overlay in dark territory, compared to that territory with TCS, if the new system is to be used to replace TCS, or where CTC might be expected), has analyzed all unique elements of the system, and has analyzed key variables, which include but are not limited to:

—Operational rules including any timetable special instructions, yard limit rules, flagging rules, to the extent they differ and are applicable to the subdivisions being considered. This is especially important when generalizing from one railroad to a second, or between subdivisions of a railroad, which incorporate different methods of operation;
—Terrain (curvature and grade);
—Radio coverage, especially if affected by different terrain;
—Number of train moves including turnaround locals and foreign traffic;
—Train weight;
—Train lengths;
—Speed;
—Complexity of Operation;
—Relevant signal and train control safety-critical appliances (*e.g.*, components and subsystems of various functional types); and
—Other conditions that relate to risk assessment, especially those that cause changes in key assumptions in the risk assessment.

In reviewing a generalized assessment FRA will consider whether the system has actually been deployed, and how well actual operating experience conforms to model predictions. FRA will give tighter scrutiny to models attempting to generalize where there is no actual operating experience, and will expect more convincing data to show with a high degree of confidence that the proposed system will be at least as safe as what it would replace.

During the discussion of the base case issue with the Working Group, post NPRM, it became evident that a significant portion of the concern with respect to triggers for adjustment of the base case had to do with the complex circumstances surrounding the transition from signal-based methods of operation to methods of operation utilizing cab displays and intervention to mitigate risk. Members of the Working Group suggested that the rule address the implications of discontinuance or material modifications of signal systems under part 235 in the final rule. FRA understood the need to address the issue and does so in a new paragraph at the end of § 236.909.

The new provision presents three situations that are foreseeable as railroads seek approval of discontinuance and material modifications under part 235 and of PSPs under the new subpart H. Section 236.911(b) provides that FRA may consolidate handing of these two proceedings. The first situation is one where the part 235 application supports a discontinuance or material modification, without regard to protections for safety in the PSP. The obvious extension of the principles developed in this rulemaking is that the previous condition would be that allowed following the grant of the discontinuance or material modification. Thus, in a typical case the railroad would have broad latitude to implement the PSP.

The second situation is one where FRA determines that the part 235 application should be denied. In that case, the previous condition would not be subject to adjustment, and the PSP would be evaluated against the actual level of safety on the territory.

The third situation is one where both outright approval and outright denial appear inappropriate given the existing situation on the territory and the pendency of the request for PSP approval. The new provision says that FRA will consider whether the proposed actions, taken as a whole, are consistent with safety and in the public interest. These are the same criteria applicable to waiver of existing FRA standards. It is possible to envisage a case where the railroad's case for discontinuance is rather strong (*e.g.*, the system is very old, costly to maintain, and the current traffic is light), but not quite sufficient to warrant granting relief. At the same time, the railroad wishes to extend an existing train control system into the territory with initial, minimal equipment on the wayside but a significant reduction in the cost of maintenance. Traffic might be projected to remain low for the foreseeable future; but the railroad might wish to ensure flexibility for future traffic growth (see § 236.907(a)(2)). In this example, the existing signal system and the new train control system (relying principally on on-board apparatus already on locomotives) might appear to provide approximately equal safety, but the degree of uncertainty associated with the analysis might prevent the FRA decision maker from having a high degree of confidence that this is the case. In this example, FRA might elect to allow the discontinuance predicated on installation of the new train control system with or without conditions (such as the requirement to monitor heavily used switches), recognizing that (i) harvesting the potential benefits of communication-based train control systems requires widespread application, and (ii) maintaining the existing system might impose an undue hardship given the available alternative. From a formal standpoint, in such a case FRA might recognize a base case slightly below the existing level of safety; however, FRA would not be required to do so. This is consistent with the broad discretion afforded to the former ICC and to FRA under the Signal Inspection Act, and subsequent codified law, to balance public interest considerations and reach practical outcomes. *See* 49 U.S.C. 20502.

Delineating more precisely what outcomes may be appropriate in such cases is not possible given the wide variety of considerations that may apply as technology and railroad operations evolve. Further, FRA policy regarding the retention of signal systems has not been, and cannot expect to be, static; rather, that policy may evolve as railroad operations evolve, operating rules are refined, related hazards are addressed (*e.g.*, broken rails), and other readily available options for risk reduction emerge and become more affordable.

Section 236.911 Exclusions

Paragraph (a) provides that the subpart does not apply to products in service as of May 6, 2005. Railroads employ numerous safety-critical products in their existing signal and train control systems. These existing systems have proven to provide a very high level of safety, reliability, and functionality. FRA believes it would be a tremendous burden on the rail industry to apply this subpart to all existing systems, which have to date proven safe.

FRA received one comment contending that existing solid state equipment should not be grandfathered. FRA disagrees with the commenter and believes the safety record of this equipment is good and does not warrant the burden necessary to essentially re-prove that it is safe.

Another commenter inquired whether products with a proven track record in the light rail or transit industry would be excluded from the new requirements. Similarly, one commenter wanted clarification that the exclusion would apply to signal and train control products in service, in freight or passenger railroad applications internationally, regardless of where in the world the products are installed.

FRA was unable to fashion an outright exclusion from subpart H requirements for equipment previously used in transit and foreign service. FRA does not have the same degree of direct access to the service history of these systems. Transit systems, except those that are connected to the general railroad system, are not directly regulated by FRA at the national level. FRA's experience with eliciting safety documentation from foreign authorities has not been good, particularly given the influence of national industrial policies.

However, FRA does believe that the potential exists for simplification of the PSP process (rather than an exclusion from the process) under which the railroad and supplier could establish safety performance at the highest level of analysis for the particular product, relying in part on experience in the other service environments and showing why similar performance should be expected in the U.S. environment. International signal suppliers should be in a good position to marshall service histories for these products and present them as part of the PSP. Whether working within subpart H or in a waiver context, the applicant(s) should address additional issues such as the following:

1. Detailed description of the change, the associated affected components, functional data flow changes, and any changes associated with safety capabilities of the product.

2. The analysis used to verify that the change did not introduce any new safety risks, or if potential risks were added, the risks and their mitigation.

3. The tests plan and associated results used to verify and validate the correct functionality of all modes of the safety-related capabilities of the product with the component refreshed.

4. Identification of any changes in training, test equipment, or maintenance required for the continued safe operation of the product.

Paragraph (b) addresses the products that are designed in accordance with part 236, subparts A through G, not in service at present but which will be in the developmental stage or completely developed prior to publication of this rule. The Standards Task Force prior to publication of the NPRM felt that these products ought to be excluded from the requirements of subpart H upon notification to FRA by 60 days after publication of the rule, if the product were placed in service by 3 years after publication of the final rule. FRA agrees that, at least for products that will be placed in service within three years of issuing this rule, it will be too costly for the railroads and suppliers to re-do work and analysis for a product on which development efforts have already begun. Similarly, it would be unfair to subject later implementations of such technology to the requirements of subpart H. In addition, FRA believes that railroads ought to be given the option to have products which are excluded made subject to subpart H by submitting a PSP and otherwise complying with subpart H. FRA has therefore adopted a provision providing this option.

Paragraph (c) addresses the exclusion of existing and future deployments of existing office systems technology. Currently, some railroads employ these dispatch systems as part of their existing signal and train control systems. These existing systems have been implemented voluntarily to enhance productivity and have proven to provide a reasonably high level of safety, reliability, and functionality. It would be a tremendous burden on the rail industry to apply subpart H to this technology and, in the case of smaller railroads, might discourage its use. The Standards Task Force recommended at the NPRM stage that a subsystem or component of an office system must comply with subpart H if it performs safety-critical functions within a new or next-generation signal and train control system. FRA agrees with this recommendation and further feels that this requirement assures the safe performance of the system.

Paragraph (d) establishes requirements for modifications of excluded products. At some point changes to excluded products qualified as significant enough to require the safety assurance processes of subpart H to be followed. This point exists when a change results in degradation of safety or in a material increase in safety-critical functionality. FRA received a comment to the NPRM inquiring whether product modifications caused by implementation details might cause products that were previously excluded from subpart H to be covered by subpart H requirements. FRA believes that modifications caused by implementation details will not necessarily cause the product to become subject to subpart H. These types of implementation modifications will be minor in nature and be the result of site specific physical constraints. FRA expects that implementation modifications that will result in a degradation of safety or a material increase in safety-critical functionality, like a change in executive software, will cause the product to be subject to subpart H and its requirements.

Paragraph (e) clarifies the application of subparts A through G to products excluded by this section.

Section 236.913 Filing and Approval

This section describes the railroad's requirements for notifying FRA of its preparation of a PSP to ensure compliance with procedures established in the RSPP and the requirements of this subpart.

Paragraph (a) establishes a requirement for preparation of a PSP for each product covered by this subpart, and discusses the circumstances under which a joint PSP must be prepared. A joint PSP must be prepared when (1) the territory on which a product covered by the subpart is normally subject to joint operations, or is operated upon by more than one railroad; and (2) the PSP involves a change in the method of operations. ''Normally subject to joint operations'' is intended to mean any territory over which trains are regularly operated by more than one railroad. FRA does not intend to require a joint PSP for territory over which trains are re-routed on an emergency basis, unless there are other, scheduled trains conducted over this territory by more than one railroad. Railroads have expressed concern that this standard may be too restrictive if it includes any territory over which more than one railroad has operating rights. However, where a railroad has operating rights over a territory where a new train control system will be installed, that

railroad's locomotives will need to be appropriately equipped or the PSP will need to show that safety is not degraded from the previous condition.

FRA invited comments specifically addressing this issue, and received comments on the subject. Commenters seemed concerned with having a clear distinction between situations where a single railroad would submit a PSP, where a joint PSP would be required, or when a PSP could be used more than once. If for example, a railroad plans to install a new signal system utilizing next-generation processor-based technology, the owning railroad alone will submit a PSP. This example assumes that other railroads using the host railroad's trackage will not need specially equipped locomotives. In situations where the host railroad's installation will require train control compatibility such as specially equipped locomotives, a joint PSP will be required.

In addition to this distinction, comments explored the concept of using the same PSP for different applications or perhaps even different railroads. The concept of having a ''portable'' PSP was actively discussed by the Working Group both before and after publication of the NPRM. FRA can foresee circumstances where the original PSP submitted has a scope sufficient to cover a new application of the product. In those instances, a railroad is invited to submit its previously approved PSP along with a cover letter delineating its new, yet comparable use. In addition to this scenario, FRA can foresee an instance where a supplier has designed a system or product under the most challenging restrictions, anticipating various operating conditions, such that the PSP could be used for different railroads. (See, also, discussion of ''generalizability,'' above.)

In paragraph (b), FRA establishes a two-tiered approach where some products require an informational filing, while others will necessitate full FRA review and approval by petition. The railroad must submit a petition for approval only when installation of new or next-generation train control systems is involved. During the course of its deliberations, prior to issuance of the NPRM, the Standards Task Force developed a matrix of railroad actions regarding processor-based signal and train control systems and the level of FRA scrutiny that ought to be required. Eventually, the group whittled this matrix down to three situations for which the railroad must petition the FRA for approval. These were: (1) Any installation of a new or next-generation train control system; (2) any replacement of an existing PTC system with a new or next-generation train control system, and (3) any replacement of an existing PTC system with an existing PTC system. All other situations would require an informational filing, subject to the procedures proposed in § 236.913(e). The Standards Task Force recommended to the Working Group at the NPRM stage that existing processor-based train control systems should be subject to the requirements of § 236.911, and the recommendation was reflected in RSAC's recommendation to FRA, so the third situation was no longer considered subject to petition procedures. Also, since the second situation is a subset of the first, only one situation remains for which a petition for FRA approval is required. FRA agrees with the RSAC recommendation and the NPRM provided, that review and approval is required for all installations involving new or next-generation train control systems; mere informational filings will not be sufficient in this case. FRA sought comments specifically addressing when petitions should be required in lieu of informational filings but no comments were submitted. The rule language remains the same. In addition, some changes requiring a PSP are most appropriately combined with modifications made in accordance with part 235. Any product change or implementation needs an informational filing at a minimum. Paragraph (b) also states that some issues may be addressed through FRA's waiver process in part 211.

Paragraph (c) specifies procedures for submitting informational filings. Informational filings are less formal and detailed than full petitions for approval, and FRA will in most instances merely audit to determine whether the railroad has followed the requirements established in subpart H and the railroad's RSPP. Since this process is expected to be less complicated and formal than a full petition for approval review, FRA anticipates being able to respond within 60 days. The railroad must identify where the PSP is physically located since FRA may want to inspect it during normal business hours. This might alleviate any FRA concerns, negating the need for treating the informational filing as a petition for approval. FRA included in the NPRM general criteria for situations in which FRA will require an informational filing to be upgraded to a full petition for approval. That criteria has been carried forward to this final rule. FRA believes these filings will be upgraded only for good cause, and gives examples of what will be considered good cause. Although FRA invited comment regarding the issue of good cause, no comments were submitted addressing the subject.

Paragraph (d) addresses requirements for petitions for approval. FRA classifies petitions for approval into two categories: those involving prior FRA consultation (covered in paragraph (d)(1)) and those that do not (covered in paragraph (d)(2)). In this rule, FRA does not require prior consultation but attempts to accommodate railroads' often tight development and implementation schedules by getting involved early. Optimally, FRA feels it should be involved at the system design review phase of development, thereby reducing the scope of FRA review which might otherwise be required. FRA believes that a railroad's failure to involve FRA early enough in the process could potentially delay FRA approval and system implementation. This rule invites the railroad to garner government involvement at an early stage in the development of a product requiring a petition for approval or a product change for which a petition for approval is required. Paragraph (d)(1) concerns petitions for approval involving prior FRA consultation. Under this procedure, FRA issues a letter of preliminary review within 60 days of receiving the Notice of Product Development. This process allows FRA to more easily reach a decision on a petition for approval within 60 days of receipt.

Paragraph (d)(2) concerns petitions for approval which do not involve prior FRA consultation. When railroads wait to involve FRA until they are approaching use of the system in revenue service, paragraph (d)(2)(iii) specifies that the agency will attempt to act on the petition within 180 days of filing. If FRA does not act on the petition within 180 days it will notify the petitioner as to why the petition remains pending. FRA believes that railroads should be encouraged to take necessary safety assurance steps to cure a petition of any apparent inadequacies before FRA requires a third party review. FRA received comments addressing the possibility of a conditional approval pending results of non-critical data inputs or in the alternative shorter FRA response periods for less complex products or changes. FRA suggests that railroads indicate a targeted date and the relevance of that date when making their filing so that FRA knows immediate action is needed. FRA will endeavor to meet requested dates, since

it is unlikely that the agency will need 180 days in all cases.

Paragraph (e)(1) establishes a role for product users in the review process. FRA believes comments from employees who will be working with products covered by this subpart will provide useful safety insight. Accordingly, FRA will consider them to the degree practicable.

Paragraph (e)(2) requires that FRA provide notice to the public of pending filings and petitions. This method of notice will allow local, national and international labor organizations to get involved with issues of interest. FRA believes that information provided by organizations whose members work directly with or will work directly with products subject to this subpart is important. FRA will consider any information it receives to the degree practicable, when involved in the review of informational filings and petitions for approval.

Paragraph (f) allows railroads to file petitions for approval prior to field testing and validation of the product. The petition for approval process must provide information necessary to allow FRA involvement in monitoring of the test program. FRA encourages railroads to avail themselves of this provision so as to provide FRA with notice of the product development earlier rather than later in the development process.

Paragraph (g) describes the approval process of a PSP. A PSP gains approval when the requirements listed in paragraph (g)(1) have been met.

Paragraph (g)(2) lists the factors which FRA will consider when evaluating the railroad's risk assessment. As the Standards Task Force toiled with this subject (pre-NPRM) it was felt that some guidance or acknowledgment of what factors would be considered by FRA during this process should be spelled out. Paragraph (g)(2)(i) explains that FRA will consider the product's compliance with recognized standards in product development. Factors such as the use of recognized standards in system design and safety analyses, accepted methods in risk estimates and proven safety records for proposed products will tend to simplify FRA's review. Paragraph (g)(2)(iii) states that FRA will consider as a factor the overall complexity and novelty of the product design. Railroads have indicated that this factor appears to be a barrier to innovation. Although FRA invited comment on this subject, no comments were submitted. Paragraph (g)(2)(vii) lists as a factor whether or not the same risk assessment method was used for both the previous condition and the risk calculation for the proposed product. FRA feels that this is important because risk assessment methods vary widely in nature. A common characteristic is their ability to describe relative differences in risk associated with changes in the environment, rather than predicting absolute values for future safety performance. However, railroads have indicated their belief that so long as the methods are acceptable to FRA, it should not matter whether a different one was used. FRA specifically sought comments addressing whether factor (vii) ought to be included as a factor either in the PSP approval decision or the decision to recommend a third-party assessment. No comments were submitted on these subjects.

Paragraph (g)(3) discusses additional factors FRA considers in its decision concerning use of the product by the railroad. Paragraph (g)(4) indicates that FRA is not limited to either granting or denying a petition for approval as is, but rather may approve it with certain conditions. Paragraph (g)(5) includes the provision that FRA be able to reopen consideration of a petition for cause and sets forth potential reasons for reopening, including such circumstances as credible allegation of error or fraud, assumptions determined to be invalid as a result of in-service experience, or one or more unsafe events calling into question the safety analysis underlying the approval.

Paragraph (h) establishes factors considered by FRA when requiring a third-party assessment and specifies who qualifies as an independent third party. FRA received a general comment suggesting that third-party assessments be required only once for each product, no matter where implemented. The answer to this question will likely be determined by whether the PSP itself has been structured to foster ''portability.''

Paragraph (h)(1) lists those factors recommended by RSAC at the NPRM stage and adopted by FRA, many of which are the same used in deciding whether to approve a PSP. This list provides guidance to product developers for criteria they would be expected to meet to avoid the prospect of a third party assessment.

Paragraph (h)(2) defines the term ''independent third party'' as initially adopted by FRA in the NPRM. FRA may maintain a roster of recognized technically competent entities, as a service to railroads selecting reviewers under this subpart. Interested parties may submit credentials to the Associate Administrator for Safety for consideration to be included in such a roster. Prior to publication of the NPRM, railroads indicated concern that the definition is unduly restrictive because it limits independent third parties to ones ''compensated by'' the railroad or an association on behalf of one or more railroads that is independent of the supplier of the product. FRA believes that requiring the railroad to compensate a third party will heighten the railroad's interest in obtaining a quality analysis and will avoid ambiguous supplier/third-party relationships that could indicate possible conflicts of interest. FRA sought comment on this subject but received none.

Paragraph (h)(3) explains that the minimum requirements of a third party audit are outlined in Appendix D and that FRA limits the scope of the assessment to areas of the safety validation and verification which deserve scrutiny. This will allow reviewers to focus on areas of greatest safety concern and eliminate any unnecessary expense to the railroad. In order to limit the number of third-party assessments, FRA first strives to inform the railroad as to what portions of a submitted PSP could be amended to avoid the necessity and expense of a third-party assessment altogether.

Paragraph (i) addresses handling of PSP amendments. The procedures which apply to notifying FRA of initial PSPs also apply to PSP amendments. However, PSP amendments may take effect immediately if they are necessary in order to mitigate risk, and if they affect the safety-critical functionality of the product. During discussions for the NPRM, the Standards Task Force recommended to the Working Group that a more informal process is warranted in order to alleviate safety concerns which are discovered after FRA is notified of the initial PSP. Discussions prior to issuance of the NPRM included consideration of a rule which would allow for all PSP amendments to be handled via informational filing; however, FRA felt that the same concerns which apply to initial filing (either as a petition or as an informational filing) should apply to the PSP amendment. No comments were submitted addressing this section and the rule remains the same.

Paragraph (j) identifies procedures for obtaining FRA approval to field test a subpart H product. FRA approval is necessary where the railroad seeks to test any product for which it would otherwise be required to seek a waiver for exemption of specific part 236 regulations. For instance, when field testing of the product will involve direct interface with train crew members, there may be a requirement for some control mechanisms to be in place. Also,

railroads will likely need to test products for operational concepts and safety-critical consideration of the product prior to implementation. This paragraph provides an alternative to the waiver process when only part 236 regulations are involved. When regulations concerning track safety, grade crossing safety, or operational rules are involved, however, this process would not be available. Such testing may also implicate other safety issues, including adequacy of warning at highway-rail crossings (including part 234 compliance), qualification of passenger equipment (part 238), sufficiency of the track structure to support higher speeds or unbalance, and a variety of other safety issues, not all of which can be anticipated in any special approval procedure. ''Clearing the railroad'' for the test train answers only a portion of these issues. Typically, waiver proceedings under part 211 allow a forum for review of all relevant issues. Based on available options, FRA would foresee the need to continue this approach in the future. FRA sought comment on its view, but no comments were submitted addressing this issue. Under this paragraph, railroads may also integrate this informational filing with the filing of a petition for approval or informational filing involving a PSP. The information required for this filing, as described in paragraphs (j)(1)–(j)(7), is necessary in order for FRA to make informed decisions regarding the safety of testing operations.

Section 236.915 Implementation and Operation

This section establishes minimum requirements, in addition to those found in the PSP, for product implementation and operation.

Paragraph (a) establishes requirements relating to when products may be implemented and used in revenue service. Paragraph (a)(1) discusses the standard for products which do not require FRA approval, but rather an informational filing. Paragraph (a)(2) addresses the standard for products which require that a petition for approval be submitted to FRA for approval. Such products shall not be used in revenue service prior to FRA approval. Paragraph (a)(3) excepts from the requirements of paragraphs (a)(1) and (a)(2) those products for which an informational filing had been filed initially, then FRA elected after implementation to treat the filing as a petition for approval. In the case where FRA chooses to treat an informational filing as a petition for approval after implementation, ''for cause'' is not intended to be restricted to the same interpretation given in § 236.913(c) for ''good cause.'' FRA envisions that cause for review after implementation will more likely be related to actual in-service performance than initial design safety considerations.

Paragraph (b) establishes a requirement that railroads will not exceed maximum volumes, speeds, or any other parameter limit provided for in the PSP. On the other hand, a PSP could be based upon speed/volume parameters that are broader than the intended initial application, so long as the full range of sensitivity analyses are included in the supporting risk assessment. FRA feels this requirement will help ensure that comprehensive product risk assessments are performed before products are implemented. This paragraph also makes allowance for amendment of PSPs even after implementation. Railroads indicated they will need the ability to amend PSPs to correct initial assumptions after implementation. Furthermore, railroads feel that if operating conditions for which a product was designed are no longer applicable and safety levels have not been reduced, the necessary corresponding PSP amendments should be allowed. FRA agrees that a mechanism must be available to handle this kind of circumstance, but of course the degree of scrutiny afforded the amendment would depend upon the specific risk profile of the proposed change.

Paragraph (c) requires that each railroad ensure the integrity of a processor-based system not be compromised, by prohibiting the normal functioning of such system to be interfered with by testing or otherwise without first taking measures to provide for the safety of train movements, roadway workers, and on-track equipment that depend on the normal functioning of the system. This provision parallels current § 236.4, which applies to all devices. By requiring this paragraph, FRA merely intends to clarify that the standard in current § 236.4 applies to subpart H products.

Paragraph (d) requires that, in the event of the failure of a component essential to the safety of a processor-based system to perform as intended, the cause be identified and corrective action taken without undue delay. The paragraph also requires that until repair is completed, the railroad be required to take appropriate measures to assure the safety of train movements, roadway workers, and on-track equipment. This requirement mirrors current requirement § 236.11, which applies to all signal system components.

Section 236.917 Retention of Records

Paragraph (a) identifies the documents and records the railroad is required to maintain at a designated office on the railroad. All documents and records must be available for FRA inspection and copying during normal business hours. The following records are required to be maintained for the life-cycle of the product. First, the railroad needs to maintain adequate documentation to demonstrate that the PSP meets the safety requirements of the RSPP and applicable standards in this subpart, including the risk assessment. The risk assessment must contain all initial assumptions for the system that are listed in paragraph (i) of Appendix B—Risk Assessment Criteria. Second, the product Operations and Maintenance Manual, as described in § 236.919, needs to be kept for the life-cycle of the product. The railroads are also required to maintain training records which designate persons who are qualified under § 236.923(b); these records will be kept until new designations are recorded or for at least one year after such person(s) leave applicable service. Paragraph (a) also requires that implementation, maintenance, inspection, and testing records as described in § 236.907(a)(18)(ii) be recorded as prescribed in § 236.110.

During Working Group discussions, railroads have indicated concerns that the product life-cycle is too long a term to keep the data proving PSP compliance with the RSPP. FRA is sympathetic to this concern but wishes to ensure that all records relevant to the current configuration and operation of the system remain available. FRA sought comments specifically concerning this issue, but received none. FRA has slightly revised the language to clarify that the timing of retention of training records is governed by § 236.923(b).

After the product is placed in service, paragraph (b) requires the railroad to maintain a database of safety-relevant hazards as described in § 236.907(a)(6), which occur or are discovered on the product. This database information shall be available for inspection and replication by FRA and FRA certified state inspectors, during normal business hours. Paragraph (b) also provides the procedure which must be followed if the frequency of occurrence for a safety-relevant hazard exceeds the threshold value provided in its PSP. This procedure involves taking immediate steps to reduce the frequency of the hazard and report the hazard occurrence to FRA. FRA realizes the scope and

difficulty of undertaking these actions could vary dramatically. In some cases, an adequate response could be completed within days. In other cases the total response could take years, even with prompt, deliberate action. If the action were to take a significant time, FRA would expect the railroad to make progress reports to FRA.

The reporting requirement of § 236.917(b) is not intended to excuse lack of compliance with current reporting requirements of part 233. In the case of a false proceed signal indication, FRA would not expect the railroad to wait for the frequency of such occurrences to exceed the threshold reporting level assigned in the hazard log. Rather, current § 233.7 requires *all* such instances to be reported.

FRA notes that the Standards Task Force recommended to the Working Group and FRA agreed that railroads take prompt countermeasures to reduce only the frequency of the safety-relevant hazard; this recommendation was incorporated in RSAC's recommendation to FRA in the NPRM. There may be situations where reducing the severity of such hazards will suffice for an equivalent reduction in risk. For example, reducing operating speed may not reduce the frequency of certain hazards involving safety-critical products, but it would in most cases reduce the severity of such hazards. FRA invited comments specifically addressing this issue, and received a comment suggesting that the rule retain its flexibility in risk management methodology. Another comment contended that severity may be hard to predict, since there will likely not be enough incidents to make an accurate prediction based on an average. The commenter agreed with FRA that there may be instances where severity in any given incident may be higher than expected. The rule is unchanged from the NPRM.

During Working Group discussions (pre-NPRM) the concern emerged that 15 days is not enough time to be held to report any inconsistency to FRA, especially when traditional postal service is used to deliver the report. As such, railroads proposed that they be given 30 days to report any inconsistencies. The NPRM permitted railroads to fax or e-mail reports of inconsistencies, which would relieve concerns about traditional postal service. FRA currently allows faxing or e-mailing of reports required by §§ 233.7 and 234.9, involving signal failure and grade crossing signal system failure, respectively. Commenters were invited to address this issue, and FRA received one comment concluding that 15 days is sufficient. FRA has amended the rule text to explicitly provide for reporting in writing by mail, facsimile, e-mail, messenger, or hand delivery. Documents that are hand delivered to FRA must not be enclosed in an envelope, as all envelopes are required to be routed through the DOT mail room.

Section 236.919 Operations and Maintenance Manual

This section requires that each railroad develop a manual covering the requirements for the installation, periodic maintenance and testing, modification, and repair for its processor-based signal and train control systems. At the NPRM stage the Standards Task Force recommended to the Working Group that railroad employees working with safety-critical products in the field have a manual with complete and current information for installation, maintenance, repair, modification, inspection, and testing of the product being serviced; the recommendation was incorporated in RSAC's recommendation to FRA and adopted by FRA in the NPRM. FRA received several comments generally addressing this section. Commenters expressed concern about the significant volume of paper resulting from this requirement. Comments provided alternatives to a written manual such as a computer disc or other electronic format. FRA acknowledges that an electronic format is an appropriate medium for such a manual. Electronic copies of the manual should be maintained in the same manner as other electronic records, and the manual should be included in the railroad's configuration management plan (with the master copy and dated amendments carefully maintained so that the status of instructions to the field as of any given date can be readily determined).

Paragraph (a) works with §§ 236.905 and 236.907 and requires that all specified documentation contained in the PSP necessary for the installation, repair, modification and testing of a product be placed in an Operations and Maintenance Manual for that product and be made available to both persons required to perform such tasks and to FRA.

Paragraph (b) requires that plans necessary for proper maintenance and testing of products be correct, legible, and available where such systems are deployed or maintained. The paragraph also requires that plans identify the current version of software installed, revisions, and revision dates.

Paragraph (c) requires that the Operations and Maintenance Manual identify the hardware, software, and firmware revisions in accordance with the configuration management requirements specified in the PSP.

Paragraph (d) requires that safety-critical components contained in processor-based systems, including spare equipment, be identified, replaced, handled, and repaired in accordance with the configuration management requirements specified in the PSP.

Section 236.921 Training and Qualification Program, General

This section sets forth the general requirements of an employer's training and qualification programs related to safety-critical processor-based signal and train control products. This section works in conjunction with § 236.907, which requires the PSP to provide a description of the specific training necessary to ensure the safe installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product. This section does not restrict the employer from adopting additional or more stringent training requirements. The training program takes on particular importance with respect to safety-critical processor-based signal and train control products, and in particular, processor-based train control products, because the railroad industry's workforce generally does not have thorough knowledge of the operation of such equipment and appropriate practices for its operation and maintenance. FRA believes employee training and qualification on how to properly and safely perform assigned duties are crucial to maintaining safe railroad equipment and a safe workplace.

FRA believes that many benefits will be gained from the railroads' investment in a comprehensive training program. The quality of inspections will improve, which will result in fewer instances of defective equipment in revenue service and increased operational safety. Under an effective training program: Equipment conditions that require maintenance attention are more likely to be discovered and repairs can be completed safely and efficiently; trouble-shooting will more likely take less time; and maintenance will more likely be completed correctly the first time, resulting in increased safety and decreased costs.

The program will provide training for persons whose duties include inspecting, testing, maintaining or repairing elements of a railroad's safety-critical processor-based signal and train control systems, including central

office, wayside, or onboard subsystems. In addition, it will include training required for personnel dispatching and operating trains in territory where advanced train control is in use and for roadway workers whose duties require knowledge and understanding of operating rules. Finally, it will include supervisors of the foregoing persons.

FRA received one comment addressing the cost of training to the railroads. This commenter believes the costs are twofold, comprised of the actual cost of training and the cost to the industry over time as computer-trained technicians leave the industry for better paying jobs with better hours. FRA believes the actual cost of training is inescapable. The burden of the initial training of the work force will be eased as employees and contractors become familiar with the equipment on which they are working. FRA believes that refresher training is less costly than initial training, and thus will ease some of the financial burden on railroads and contractors. In addition, FRA believes any projected costs based on trained technicians leaving the industry is speculative. The possibility that employees may leave any profession is always present and difficult to quantify. FRA believes the possibility of attrition is certainly no disincentive to adequately train employees for their current jobs.

Paragraph (a) establishes the general requirement for when a training program is necessary and who must be trained. Training programs must meet the minimum requirements listed in §§ 236.923 through 236.929, as appropriate, and any more stringent requirements in the PSP for the product.

FRA received a comment expressing concern that each railroad would have the responsibility of training railroad employees, contractor employees, and presumably supplier personnel. The commenter reasoned that such a task would be impossible for any given railroad. FRA wants to clarify the intent of this section. Railroads are responsible for training their own employees. Contractors, including suppliers whose employees are performing the duties described in this section, are also responsible for training their own employees. Yet, FRA is not requiring that railroads provide training for contractor employees. FRA has changed the language of the section to substitute the term ''employer'' for the term ''railroad'' to more clearly indicate that employers are responsible for having their employees who perform work covered by this section trained and qualified. If FRA finds untrained contractors performing work that requires training, both the contractor and railroad may potentially be subject to civil penalty enforcement activity. Railroads should be seeking assurance that contractors have training programs that comply with this section and that the contractors are utilizing trained and qualified personnel to perform work on a railroad's processor-based safety-critical signal and train control products. If FRA finds untrained contractor employees conducting work which requires training, FRA can proceed against both the contractor and the railroad. If the railroad has placed a clear contractual responsibility on the provider of services to train personnel and maintain appropriate records, FRA would normally proceed first against the contractor. In any event, FRA would expect to see prompt corrective action.

Paragraph (b) establishes the general requirement that the persons cited in paragraph (a) must be trained to the appropriate degree to ensure that they have the necessary knowledge and skills to effectively complete their duties related to operation and maintenance of products.

Section 236.923 Task Analysis and Basic Requirements

This section sets forth specific parameters for training railroad employees and contractor employees to assure they have the necessary knowledge and skills to effectively complete their duties as related to safety-critical products and the functioning of advanced train control systems. FRA has changed the language of the section to substitute the term ''employer'' for the term ''railroad'' to indicate that employers, whether railroads or contractors, are responsible for complying with this section. This section explains that the functions performed by an individual will dictate what type of training that person should receive related to the railroad's processor-based signal and train control system. For example, a person that operates a train would not require training on how to inspect, test, and maintain the system equipment unless the person were also assigned to perform those tasks.

The intent of this section is to ensure that employees who work with products covered by this rule, including contractors, know how to keep them operating safely. The final rule grants the employer flexibility to focus and provide training that is needed in order to complete a specific task. However, the rule is designed to prevent the employer from using under-trained and unqualified people to perform safety-critical tasks.

This section describes that the training and qualification programs specified in § 236.919 must include a minimum group of identified requirements. These minimum requirements will be described in the PSP. This required training is for railroad employees and contractor employees to assure they have the necessary knowledge and skills to effectively complete their duties related to processor-based signal and train control systems.

Paragraphs (a)(2) and (a)(3) provide that the employer will identify inspection, testing, maintenance, repairing, dispatching, and operating tasks for signal and train control equipment and develop written procedures for performance of those tasks. Paragraph (a)(4) requires that the employer identify additional knowledge and skills above those required for basic job performance necessary to perform each task. The point here is that work situations often present unexpected challenges, and employees who understand the context within which the job is to be done will be better able to respond with actions that preserve safety. Further, the specific requirements of the job will be better understood; and requirements that are better understood are more likely to be adhered to. An example is so-called ''gap training'' for employees expected to work on electronic systems. Employees need to understand in at least a general way how their duties fit into the larger program for maintaining safety on a railroad. If they lack a basic understanding of the functioning of the systems they are working on, they are more likely to make a mistake in a situation where instructions are ambiguous and where the unusual nature of the problem prompts discovery of a void in the instruction set. Well informed employees will be less likely to free-lance trouble shooting; and, incidentally, they should also be of greater value in assisting with trouble shooting (an economic benefit which should, by itself, offset the cost of the requirement).

Paragraph (a)(5) requires that the employer develop a training curriculum which includes either classroom, hands-on, or other formally-structured training designed to impart the knowledge and skills necessary to perform each task.

FRA received a comment suggesting that the rule text assumed unlimited budget allocation for training and suggested that the training curriculum should be designed by the railroad in consultation with the manufacturer of the product, utilizing training materials and manuals prepared by the vendor.

FRA does not disagree with the comment and sees nothing in the rule text that would prevent a railroad or other employer from proceeding in this manner. The employer and manufacturer's consultation would need to be conducted with the requirements of this section in its entirety in mind.

Paragraph (a)(6) establishes the requirement that all persons subject to training requirements and their direct supervisors must successfully complete the training curriculum and pass an examination for the tasks for which they are responsible. For example, a person who operates a train would not require training on how to inspect, test, or maintain the equipment unless the person were assigned to also perform those tasks. Generally, appropriate training must be given to each of these employees prior to task assignment; however, an employee may be allowed to perform a task for which that person has not received the appropriate training only if the employees do so under the direct, on-site supervision of a qualified person. Direct supervisor is intended to mean the immediate, first-level supervisor to whom the employee reports.

FRA received comments concerning the training of direct supervisors. Commenters were concerned that direct supervisors would need to complete the same training as those who install, maintain, repair, modify, inspect, and test next generation products. The Working Group considered this comment and felt that the content of supervisor training would depend upon an analysis of the supervisor's job, including his or her specific tasks. FRA agrees with this assessment and adopted the Working Group's recommendation. The identification of training goals and the task analysis required in paragraphs (a)(1) and (2) includes management goals and tasks. Managers and supervisors must be trained to carry out the functions their duties require. If a direct supervisor is in a position where he or she may have to fulfill the responsibilities or duties of a subordinate, he or she must have the requisite knowledge and training to do so. If, however, a manager or supervisor will likely never need to fulfill the duties of a subordinate, and that person is not expected to provide technical oversight for certain functions, he or she may not need to be trained on those functions. This requirement is designed to ensure that supervisors have the requisite knowledge, training, and familiarity with the duties of their subordinates such that they can competently supervise the workforce. FRA is changing the phrase ''the training curriculum'' to ''a training curriculum'' in the text of paragraph (a)(6), in order to prevent further confusion and clarify FRA's intent.

Paragraph (a)(7) requires that periodic refresher training be conducted at intervals specified in the PSP. This periodic training must include either classroom, hands-on, computer-based training, or other formally-structured training in order that railroad employees and contractor employees maintain the knowledge and skills necessary to safely perform their assigned tasks.

Paragraph (a)(8) establishes a requirement to compare actual and desired success rates for the examination. In the NPRM, FRA proposed evaluating the effectiveness of a training program by comparing the desired and actual success rates. Railroads have expressed concern about this particular requirement, during Working Group discussion and commenters were invited to address this issue. FRA received no comment. FRA believes that by stating the requirement in such a manner, it may have inadequately described the underlying purpose of the proposed rule. The objective of this requirement is twofold. The first is to determine if the training program materials and curriculum are imparting the specific skills, knowledge, and abilities to accomplish the stated goals of the training program. The second is to determine if the stated goals of the training program reflect the correct, and current, products and operations.

Over time, changes in railroad products and operations may result in differences between the original defined goals and tasks based on the original products and operations, and goals and tasks based on the current products and operations. Similarly, over time the effectiveness of the training process may change as a result of instructional methods and student skill levels. Changes in training may be necessary as a result. Ongoing, regular verification of the results of the training process is required to ensure that the training program materials and curriculum are relevant, the learning objectives are being met, and the necessary skills, knowledge and ability are actually being imparted. Without regular feedback, verification and validation (and if necessary, adjustments, to ensure the necessary relevancy and effectiveness) cannot occur. In an effort to more accurately reflect these objectives, FRA has revised § 236.923(a)(8).

Paragraph (b) provides that the employers must maintain records which designate persons who are qualified under this section. These records must be kept until new designations are recorded or for at least one year after such person(s) leave applicable service, and must be available for FRA inspection and copying.

FRA received a comment addressing the maintenance of training records. The comment expresses concern regarding the railroad's ability to maintain records of employees other than railroad employees who may be conducting work that is covered by this section on a particular railroad. As previously mentioned in the general training discussion, railroads are not being required to maintain training records for every person covered by this section who may potentially work on their property. A railroad's contractor must maintain records on contractor employees who perform work covered by this section. FRA expects to have access to the training records of contractor employees whose work functions are covered by the training requirements of this section. Early pre-NPRM discussions by the Standards Task Force involved railroads addressing these concerns when contracting. In the final rule FRA has made explicit the requirement of railroad contractors to maintain records under this section. If FRA cannot get access to such records, the railroad and contractor or supplier may be subject to civil penalty enforcement activity.

Section 236.925 Training Specific to Control Office Personnel

This section explains the training that must be provided to employees responsible for issuing or communicating mandatory directives. This training must include instructions concerning the interface between computer-aided dispatching systems and processor-based train control systems as applicable to the safe movement of trains and other on-track equipment. In addition, the training must include operating rules that pertain to the train control system, including the provision for moving unequipped trains and trains on which the train control system has failed or been cut out en route.

This section sets forth the requirements for instructions on control of trains and other on-track equipment when a train control system fails. It also includes periodic practical exercises or simulations and operational testing under part 217 to assure that personnel are capable of providing for safe operations under alternative operation methods.

Section 236.927 Training Specific to Locomotive Engineers and Other Operating Personnel

This section specifies minimum training requirements for locomotive engineers and other operating personnel who interact with processor-based train control systems. ''Other operating personnel'' is intended to refer to on-board train and engine crew members (*i.e.,* conductors, brakemen, and assistant engineers). FRA invited comments addressing the issue of whether a formal definition is needed for ''other operating personnel.'' FRA received no comment on the term and has decided to leave it undefined. Paragraph (a) requires that the training contain familiarization with the onboard processor-based equipment and the functioning of that equipment as part of a train control system and its relationship to other onboard systems under that person's control. The training program must cover all notifications by the system (*i.e.* onboard displays) and actions or responses to such notifications required by onboard personnel, as well as how each action or response ensures proper operation of the system and safe operation of the train.

Paragraph (b) states that with respect to certified locomotive engineers, the training requirements of this section must be integrated into the training requirements of 49 CFR part 240.

Paragraph (c) addresses requirements for use of a train control system to effect full automatic operation, as defined in § 236.903. FRA acknowledges that this rule is not designed to address all of the various safety issues which accompany full automatic operation (although it by no means discourages their development and implementation); however, insofar as skills maintenance of the operator is concerned, the rule offers the standards in this paragraph.

Paragraph (c)(1) establishes the requirement that the PSP must identify all safety hazards to be mitigated by the locomotive engineer.

Paragraph (c)(2) concerns required areas of skills maintenance training. The NPRM provided that training requirements can be worked out individually among the railroad, its labor representative(s), and the FRA. FRA continues to support this reasoning andnotesthat in all cases, the PSP must define the appropriate training intervals for these tasks.

FRA received one general comment on this section. The commenter appears to be seeking clarification that each railroad will have the flexibility to develop its locomotive engineer training program to be applicable to the particular system being installed by that railroad. FRA agrees that there is no one curriculum across the board that will generally satisfy the locomotive engineer training requirements. As with the general training requirements, the requisite task analysis will be specific to the functions of the system or systems of each railroad. Accordingly, the resulting training curriculum will correspond with the tasks or functions necessary for that particular system.

Section 236.929 Training Specific to Roadway Workers

This section requires the railroad to incorporate appropriate training in the program of instruction required under part 214, subpart C, Roadway Worker Protection. This training is designed to provide instruction for workers who obtain protection for roadway work groups or themselves and will specifically include instruction to ensure an understanding of the role of a processor-based train control system in establishing protection for workers and their equipment, whether at a work zone or while moving on track between work locations. Also, this section requires that training include recognition of processor-based train control equipment on the wayside and how to avoid interference with its proper functioning.

FRA received two comments addressing this section. One comment echoed previous concerns regarding the locomotive engineer training program. The commenter seemed to be seeking assurance that each railroad's roadway worker training program would be developed to apply specifically to its processor-based system. As noted earlier, FRA is not seeking compliance with any general curriculum. The required task analysis will tailor each program to the needs of the particular system to which it applies.

The second comment regarding this section suggested adding rule language to address instruction for roadway workers in case of abnormal operations. The commenter considers abnormal operations instances where there is a loss of protection provided by the processor-based system. This comment was discussed during the final meeting addressing the rule. The Working Group members referenced the language in ''236.925(c) regarding control office personnel, as possible language to use for the added requirement. FRA agrees with the commenter. FRA assumes that a good task analysis would include procedures and training on procedures for system failures. Roadway workers are uniquely situated out on the right-of-way at risk of being struck by trains and on-track equipment. Given the potential for exposure to extreme peril, FRA believes specifying training and periodic drills on that training is worthwhile. FRA is adding to paragraph (b) an additional requirement numbered paragraph (b)(3) duplicating, in part, the language of § 236.925(c).

Appendix B to Part 236—Risk Assessment Criteria

Appendix B provides a set of criteria for performing risk assessments for products sought to be implemented on a railroad. During early deliberations, prior to issuance of the NPRM, suppliers indicated concern for flexibility in performing risk assessments. FRA recognizes this concern, yet must balance it against the need for uniformity in the conduct of risk assessments performed under this subpart. This need for uniformity across all products covered by subpart H is necessary when a performance standard is sought to be used. FRA has sought to balance these two seemingly competing concerns by establishing a requirement that the risk assessment criteria be followed, but allowing for other approaches to be used if FRA agrees they are equally suitable.

Paragraph (a) addresses the life-cycle term for purposes of the risk assessment. FRA believes new signal and train control systems will be in place for at least 25 years, based on the life-cycles of current systems. Over time, these systems will be modified from their original design. FRA is concerned that subsequent modifications to a product might not conform with the product's original design philosophy. The original designers of products covered by this subpart could likely be unavailable after several years of operation of the product. FRA feels that requiring an assumption of a 25-year life-cycle for products will adequately address this problem. FRA believes this proposed criterion will aid the quality of risk assessments conducted per this subpart by forcing product designers and users to consider long-term effects of operation. However, FRA feels such a criterion would not be applicable if, for instance, the railroad limited the product's term of proposed use. In such case, FRA would only be interested in the projected risks over the projected life-cycle, even if less than 25 years.

Paragraph (a) also addresses the scope of the risk assessment for the risk calculation of the proposed product. The assessment must measure the accumulated residual risk of a signal and train control system, after all mitigating measures have been

implemented. This means that the risk calculation shall attempt to assess actual safety risks remaining after implementation of the proposed product. FRA is fairly certain that railroads proposing new products will have planned or taken measures to eliminate or mitigate any hazards which remain after the product has been designed. These might include training or warning measures. For the purpose of the risk calculation for a proposed product, FRA is interested only in residual risks, or those which remain even after all mitigating measures have been taken.

Paragraph (b) addresses the risks connected with the interaction of product components. Each signal and train control system covered by this subpart is considered to be subject to hazards associated with failure of individual components, as well as hazards associated with improper interaction of those components. FRA is aware that many unanticipated computer system faults have arisen from incomplete analysis of how components will interact. This problem is of vital importance when safety-critical systems are involved, such as those targeted by subpart H.

Paragraph (c) addresses how the previous condition is computed. The requirement mandates the identification of each subsystem and component in the previous condition and estimation of an MTTHE value for each of those subsystems and components. FRA feels that the MTTHE is an adequate measure of the reliability and safety of those subsystems and components, and it facilitates the comparison of subsystems and components which are to be substituted on a one-for-one basis (see § 236.909(d)). In some cases, current safety data for the particular territory on which the product is proposed to be implemented may be used to determine MTTHE estimates. The purpose of this provision is to require railroads to produce the basis for any previous condition calculations.

Paragraphs (d) and (e) deal with some types of risks which must be considered when performing the risk assessment. FRA believes that the listed items are relevant to any risk assessment of signal and train control systems and thus ought to be considered. However, there may exist situations when one or more of the categories of risk are not relevant, such as when a system does not involve any wayside subsystems or components. In such case, FRA would obviously not require consideration of such risks, but would expect the risk assessment to briefly explain why.

Paragraph (f)(1) addresses how MTTHE figures are calculated at the subsystem and component level. FRA feels that MTTHE should be calculated for each integrated hardware/software subsystem and component. FRA expects that quantitative MTTHE calculation methods will be used where it is appropriate and when sufficient data is available. For factors such as non-processor based systems which are connected to processor-based subsystems, software subsystems/components, and human factors, FRA realizes that quantitative MTTHE values may be difficult to assign. In these cases, the rule allows qualitative values to be used or estimated. Furthermore, for all human-machine interface components/subsystems, appropriate MTTHE estimates must be assigned. FRA feels this is necessary because an otherwise reliable product which encourages human errors could result in a dramatic degradation of safety. FRA believes this risk should be identified in the risk assessment.

Paragraph (f)(2) addresses the MTTHE estimates. The rule requires that all MTTHE estimates be made with a high degree of confidence, and relate to scientific analysis or expert opinion based on documented qualitative analysis. This paragraph also indicates the railroad must devise a compliance process which ensures that the analysis is valid under actual operating conditions. Since the relevant Standards Task Force recommendation which was the basis for the NPRM, did not provide any criteria as to how such a compliance process would be expected to operate, FRA invited comments addressing this issue. No comments were submitted. FRA has determined that each railroad will determine its own compliance process and the Appendix will remain the same.

Paragraph (g) establishes criteria for calculation of MTTHE values for non-processor-based components which are part of a processor-based system or subsystem. FRA believes that it will be common for future systems to combine processor-based components with other components, such as relay-based components. Thus, failures of non-processor-based components must be considered when determining the safety of the total system.

Paragraph (h) establishes a requirement to document all assumptions made for purposes of the risk assessment. FRA does not intend to hold the railroads to directly document these assumptions, but rather to be responsible for their documentation and production if so requested by FRA. FRA imagines that suppliers will in most cases perform the actual documenting task.

Paragraph (h)(1) addresses documentation of assumptions concerning reliability and availability of mechanical, electric, and electronic components. In order to assure FRA that risk assessments will be performed diligently, FRA requires documentation of assumptions. FRA envisions sampling and reviewing fundamental assumptions both prior to product implementation and after operation for some time. FRA intends for railroads to confirm the validity of initial risk assessment assumptions by comparing them to actual in-service data. FRA is aware that mechanical and electronic component failure rates and times to repair are easily quantified data, and usually are kept as part of the logistical tracking and maintenance management of a railroad.

Paragraph (h)(2) addresses assumptions regarding human performance. Assumptions about human performance should consider all the categories of unsafe acts as described by Reason (1990). Some methods to assess human reliability, such as the Human Cognitive Reliability model (Kumamoto and Henley, 1996, pp. 506–508), assume that unsafe acts of certain types (*e.g.*, lapses and slips) do not occur. Such a method must be supplemented with other methods, such as THERP (Technique for Human Error-Rate Prediction), that are designed to assess these unsafe acts (Kumamoto and Henley, 1996, p. 508). The hazard log required by § 236.907(a)(6) will help determine the appropriateness of the assumptions employed. This database should contain sufficient quantitative detail and narrative text to allow a systematic human factors analysis (examples of procedures to accomplish this can be found in Gertman and Black, 1994, Ch.2) to determine the nature of the unsafe acts involved and their relationship to the deployment of PTC technology, procedures and underlying factors. Thus, FRA does not intend to require railroads to maintain electronic databases solely containing human performance data. However, FRA envisions this requirement will have the effect of railroads maintaining what relevant data they can on human performance. For instance, programs of operational tests and inspections (part 217) will have to be adapted to take into consideration changes in operating rules incident to implementation of new train control systems.

Paragraph (h)(3) discusses risk assessment assumptions pertaining to software defects. FRA believes that projected risks of software failures are

difficult to forecast. Therefore, FRA feels it is important to verify that software assumptions are realistic and not overly optimistic.

Paragraph (h)(4) establishes a requirement for the documentation of identified fault paths. Fault paths are key safety risk assumptions. Failing to identify a fault path can have the effect of making a system seem safer on paper than it actually is. When an unidentified fault path is discovered in service which leads to a previously unidentified safety-relevant hazard, the threshold for defects in the PSP is automatically exceeded, and the railroad must take mitigating measures pursuant to § 236.917(b). FRA believes it is possible that railroads will encounter previously unidentified fault paths after product implementation. The frequency of such discoveries would likely be related to the quality of the railroad's safety analysis efforts. Safety analyses of poor quality are more likely to lead to in-service discovery of unidentified fault paths. Some of those paths might lead to potential serious consequences, while others might have less serious consequences. FRA is requiring the railroads to estimate the consequences of these unidentified faults as if they would continue being detected over the twenty-five year life of the product. Each product is to be treated as though it would be in service for twenty-five years from the current date, and unidentified faults would continue to be discovered at the same rate as they had been for the greater of the previous ten years in service or the life of the product. All new products are to be treated as though they had been in service for at least six months in order to prevent an early-discovered fault path from having drastic impact.

Appendix C to Part 236—Safety Assurance Criteria and Processes

During the December 2001 meeting of the PTC Working Group, a small team representing the various stakeholders and interested parties was assigned to review and address comments to Appendices C and D. The team met independently of the full PTC Working Group and presented its ideas and conclusions to the full PTC Working Group for consensus. The team recommended several changes for Appendix C, but suggested that Appendix D remain the same. The PTC Working Group reached consensus to adopt the recommended changes proposed by the team (but the full Committee failed to adopt the recommendations). FRA has elected to proceed with these changes because they add clarity and flexibility. The resulting changes are discussed with the provision of the appendix to which they apply.

Appendix C sets forth minimum criteria and processes for safety analyses conducted in support of RSPPs and PSPs. The intention of Appendix C is to provide safety guidelines distilled from proven design considerations. These guidelines can be translated into processes designed to ensure the safe performance of the product. The analysis required in Appendix C is designed to minimize failures that would have the potential to affect the safety of railroad operations. FRA recognizes there are limitations regarding how much safety can be achieved given technology limitations, cost, and other constraints. As recommended by the Standards Task Force, prior to the NPRM, FRA is establishing the objectives in the appendix, recognizing this principle.

Paragraph (a) discusses the purpose of this Appendix C. This appendix sets forth minimum criteria and processes for safety analyses conducted in support of RSPPs and PSPs. FRA is changing the language of the NPRM, in response to comments suggesting that FRA make clear that Appendix C is an informative annex, which does not set forth regulatory requirements. The text of paragraph (a)(1) is being revised to reference ''objectives'' in lieu of ''requirements.''

Paragraph (b) covers safety considerations and principles which the designer must follow unless the consideration or principle does not apply to the product. In the latter case, the designer is required to state why it believes the consideration or principle does not apply. These safety considerations and principles resulted from early discussions of the Standards Task Force, publication of the NPRM, and are recognized by the industry to be recommended practices for the development of safety-critical systems. FRA believes these proven safety considerations and concepts are a necessary starting point for the development of products under subpart H. FRA received a comment suggesting that the agency maintain and provide the most recent edition of approved validation standards. This comment was discussed at the PTC Working Group meeting. FRA decided to disregard this comment because most standards are widely available and procurement does not present a major problem. In addition, most standards are copyrighted and FRA could not reproduce them for wide dissemination.

Paragraph (b)(1) discusses design considerations for normal operation of the product. FRA notes that in normal operation, the product should be designed such that human error would not cause a safety hazard. This principle recognizes that safety risks associated with human error cannot be totally eliminated by design, no matter how well-trained and skilled the operators. FRA received a comment addressing this paragraph suggesting that compliance with this objective would be impossible. The Working Group discussed and concluded that the third sentence of this provision should be changed to read, ''Absence of specific operator actions or procedures will not prevent the system from operating safely.'' Although no formal recommendation was made by RSAC on resolution of this issue or accepted by FRA, FRA believes that the Final Rule should include this language. FRA received an additional comment on this section requesting clarification regarding the source of what constitutes an unacceptable or undesirable hazard. The Working Group discussed including a reference to MIL–STD 882 C in the final sentence of the paragraph. FRA has concluded that including such a reference in the Final Rule is appropriate and has changed the rule accordingly.

Paragraph (b)(2) addresses design considerations dealing with systematic failure. Systematic failures or errors are those that can occur when the product is poorly developed and/or the human-machine interface is not given proper design attention. FRA received a comment expressing concern that the objective of this paragraph is an absolute and un-achievable requirement. Working Group discussions concluded that the initial sentence of the paragraph should be modified to read, ''It must be shown how the product is designed to mitigate or eliminate unsafe systematic failures.'' As previously noted, no formal RSAC recommendation was made to FRA. Nevertheless, FRA believes that the discussed language is useful and has added the following to the end of the suggested sentence, ''the conditions which can be attributed to human error that could occur at various stages throughout product development.''

Paragraph (b)(3) addresses random failure. FRA recognizes hardware can fail when components fail due to wear and tear, overheating, harsh environmental conditions, etc. This consideration ensures that such hardware failures do not compromise safety. FRA received a comment expressing concern that automatic restarts may not always be optimal. Working Group discussions concluded

that the fourth sentence of the paragraph (b)(3)(i) should be modified to read, ''In the event of a transient failure and if so designed, the system should restart itself, if it is safe to do so.'' As previously noted, no formal RSAC recommendation was made to FRA. FRA has amended the Final Rule to include the Working Group language, for clarity. FRA also received a comment suggesting that paragraph (b)(3)(ii)'s objective is too restrictive and un-achievable. The Working Group concluded that use of the word ''credible'' to modify single point failures would alleviate the commenter's concern. FRA thinks the addition of that word makes good sense, and the final rule reflects that change.

Paragraph (b)(4) deals with common mode failure. The common mode failures are those that stem from a component failure that can cause other components to fail due to close association among components. These failures are due primarily to poor design practices with respect to interaction among and between components.

Paragraph (b)(5) discusses external influences. FRA notes that external influences need to be taken into account for the safety of the product. Close attention needs to be given to the environment in which the equipment operates.

Paragraph (b)(6) addresses product modifications. In addition to PSP requirements and other relevant requirements of subpart H, close attention needs to be given as to how these modifications affect safety when modifications are made.

Paragraph (b)(7) deals with software design. Software integrity is crucial to the safety of the product. Non-vital (or non-fail-safe) components need to be controlled in such a manner so their failure does not create a hazard. For example, if a semiconductor's memory fails, software checks into the semiconductor locations can determine if a potential data corruption has occurred and take appropriate action so that the corrupted data does not constitute a hazard. Hence the importance of software design for the software controlling these types of components.

Paragraph (b)(8) addresses the closed loop principle. Closed loop means that a system is designed so that its output is continuously compared with its input to determine if an error has occurred.

FRA added a separate paragraph (9) in this appendix specifically to discuss human factors design considerations. Human-centered design principles recognize that machines can only be as effective as the humans who use them. The goals of human factors requirements and concepts in product design are to enhance safety, increase the effectiveness and efficiency of work, and reduce human error, fatigue, and stress. Since the implementation of any new system, subsystem or component can directly or indirectly change the nature of tasks that humans perform, both negative and positive consequences of implementation should be considered in design. FRA believes that these principles need to be adequately addressed early in the product development stage rather than at the end of it. Often times, an engineer or evaluator unfamiliar with human factors issues will attempt to address human factors issues as the end of the product development stage nears, at which point only changes in the way the product is implemented are possible (*i.e.*, accommodating changes in operations, additional training, etc.). Thus, FRA envisions compliance with this paragraph to be satisfied with consideration of input from a qualified human factors professional as early as possible in the development process. In addition, FRA believes that compliance with the principles set forth in Appendix E is essential to address the agency's human factors concerns.

Paragraph (c) provides that certain listed standards may be used for verification and validation procedures. These standards are already current industry/consensus standards.

Appendix D to Part 236—Independent Review and Assessment of Verification and Validation

Paragraph (a) discusses the purpose of an independent third party assessment of product verification and validation. FRA described some of the background for the requirement in the NPRM.

The requirement for an independent third party assessment is a reasonably common one in the field of safety-critical electronic systems. FRA's experience with emerging systems suggests that this approach can enhance the quality of decision making by railroads and FRA in several ways.

First, if those who design and produce electronic systems know that they may face a third party review, they will be more rigorous in creating and maintaining safety documentation for their systems. Suppliers know that FRA has limited technical assets to devote to this kind of effort, and documentation of safety engineering practice has in some instances been lacking in the past. Documentation, by itself, will not ensure a safe system. However, the absence of documentation will make it virtually impossible to ensure the safety of the system throughout its life-cycle; and this rule allows technical risks much greater than those previously managed by railroads and FRA in the past.

Second, a third-party assessment will help FRA make well informed decisions in those cases where approval of the PSP is required. The third party brings a perspective independent of the designer and allied with the interest of the railroad in ensuring the system is safe. The third party also brings a level of technical expertise that may not be available on the staff of the railroad—in effect, permitting the railroad (and thus FRA) to look behind claims of the vendor to actual engineering practice.

Third, because the third-party review can be conducted in phases as the product is specified, designed, and produced, the review should be available to the railroad and FRA as the PSP is submitted, avoiding delay associated with iterative inquiries by FRA.

Finally, where the system in question utilizes a novel architecture, relies heavily on COTS hardware and software, or is offered to replace an existing system that is highly competent, third-party review will permit a more highly refined evaluation of the MTTHE estimates which are the raw material for the system risk assessment. Very often these estimates will be critical to review of the system.

The NPRM offered specific criteria for determining whether a third-party assessment ought to be performed, and these are carried forward in the final rule. See § 236.913(h).

Paragraphs (c) through (f) discuss the substance of the third-party assessment. This assessment should be performed on the system as it is finally configured, before revenue operations commence, and requires the reviewer to prepare a final report. A typical assessment can be divided into four levels as it progresses: the preliminary level, the functional level, the implementation level, and the closure level.

Paragraph (c) addresses the reviewer's tasks at the preliminary level. Here, the assessor reviews the supplier's processes as set forth in the documentation and provides comments to the supplier. The reviewer should be able to determine vulnerabilities in the supplier's processes and the adequacy of the RSPP and PSP as they apply to the product. ''Acceptable methodology'' is intended to mean standard industry practice, as contained in MIL–STD–882C, such as hazard analysis, fault tree analysis, failure mode and effect criticality analysis, or other accepted applicable methods such as fault

injection, Monte Carlo or Petri-net simulation. FRA is aware of many acceptable industry standards, but usage of a less common one in PSP analysis would most likely require a higher level of FRA scrutiny. In addition, the reviewer considers the completeness and adequacy of the required safety documents, including the PSP itself.

Paragraph (d) discusses the reviewer's tasks at the functional level. Here, the reviewer will analyze the supplier's methods to establish that they are complete and correct. First, a Preliminary Safety Analysis is performed in the design stage of a product. In addition to describing system requirements within the context of the concept of operations, it attempts, in an early stage, to classify the severity of the hazards and to assign an integrity level requirement to each major function (in conventional terms, a preliminary hazard analysis).

Traditional methodology practices widely accepted within industry and recognized by military standard MIL–STD–882C include: Hazard Analysis, Fault Tree Analysis (FTA), Failure Mode and Effects Analysis (FMEA), and Failure Modes, Effects, and Criticality Analysis (FMECA).

Hazard analysis is an extension of the PHA performed in the later phases of product development. This hazard analysis focuses more on the detailed functions of the product and its components. A hazard analysis can be repeated as needed as the product matures. A competent safety assessor should be able to determine if sufficient hazard analyses were performed during the product development cycle.

FTA starts with an identification of all hazards and determines their possible causes. Data from earlier incidents can also be used as a starting point for the analysis. This method concentrates on events that are known to lead to hazards.

FMEA considers the failure of any component within a system, tracks the effects of the failure and determines its consequences. FMEA is particularly good at detecting conditions where a single failure can result in a dangerous situation; however, its primary drawback is that it doesn't consider multiple failures. FMEA involves much detailed work and is expensive to apply to large complex systems. FMEA is usually used at a late stage in the development process, and is applied to critical areas, rather than to the complete system. FMECA is an extension of FMEA that identifies the areas of greatest need. The above descriptions are taken from ''Safety-Critical Computer Systems'' (Storey, Neil; Addison-Wesley Longman (Harlow, England 1996), pp. 33–57.)

Other simulation methods may also be used in conjunction with the above methods, or by themselves when appropriate. These simulation methods include fault injection, a technique that evaluates performance by injecting known faults at random times during a simulation period; Markov modeling, a modeling technique that consists of states and transitions that control events; Monte Carlo model, a simulation technique based on randomly-occurring events; and Petri-net, an abstract, formal model of information flow that shows static and dynamic properties of a system. A Petri-net is usually represented as a graph having two types of nodes (called places and transitions) connected by arcs, and markings (called tokens) indicating dynamic properties.

Paragraph (e) addresses what must be performed at the implementation level. At this stage, the product is now beginning to take form. The reviewer typically evaluates the software. Most likely, the software will be in modular form, such that software modules are produced in accordance to a particular function. The reviewer must select a significant number of modules to be able to establish that software is being developed in a safe manner.

Paragraph (f) discusses the reviewer's tasks at closure. The reviewer's primary task at this stage is to prepare a final report where all product deficiencies are noted in detail. This final report may include material previously presented to the supplier during earlier development stages.

Appendix E to Part 236—Human-Machine Interface (HMI)

This appendix provides human factors design criteria. At the NPRM stage of the rulemaking, a small group of members from the Working Group comprised the Human Factors Team. The task given them was to develop comprehensive design considerations for human factors and human-machine interfaces. Their suggestions were presented as part of the recommendation to the RSAC for the NPRM. The RSAC recommendation, including the suggestions of the Human Factors Team, was accepted by FRA as part of the NPRM. Although there was no formal recommendation for a Final Rule from RSAC to FRA, FRA has based this appendix on the language provided in the NPRM. This appendix addresses the basic human factors principles for the design and operation of displays, controls, supporting software functions, and other components in processor-based signal or train control systems and subsystems. The HMI requirements in this appendix attempt to capture the lessons learned from the research, design, and implementation of similar technology in other modes of transportation and other industries. FRA has placed in the docket for this rulemaking a research document that contains a broad spectrum of references to the literature in this area.

The overriding goal of this appendix is to minimize the potential for design-induced error by ensuring that processor-based signal or train control systems are suitable for operators, and their tasks and environment. The overriding conclusion from the research is that processor-based signal or train control systems that have been designed with human-centered design principles in mind—system products that keep human operators as the central active component of the system—are more likely to result in improved safety.

Paragraph (a) addresses the purpose of the HMI requirement. The team concluded from its research that increased automation of systems through the use of products involves negative safety effects, as well as positive ones. Products with human-centered design features, however, are more likely to result in improved system safety. The human-centered systems approach recognizes that technology is only as effective as the humans who must use it. HMI designs that do not consider human capabilities, limitations, characteristics and motivation will be less efficient, less effective and less safe to operate. Therefore, the HMI requirement articulated in this appendix promotes consideration of these issues by designers during the development of HMIs.

Paragraph (b) defines two essential terms, ''designer'' and ''operator,'' which are critical to a clear understanding of the HMI requirement.

Paragraph (c) highlights various issues that designers should be aware of and attempt to prevent during the design process. For example, paragraph (c)(1) addresses ''reduced situation awareness and over-reliance,'' which can result when products transform the role of a human operator from an active system controller to a passive system monitor. Essentially, a passive operator is less alert to what the system is doing, may rely too heavily on the system and become less capable of reacting properly when the system requires the operator's attention. For that reason the HMI requirement promotes operator action to maintain operation of the equipment and provide numerous opportunities for practice. The requirement further

provides that operator action be sustained for a period of at least 30 minutes so that an operator remains involved and resistant to distraction, *e.g.,* management by consent rather than management by exception. In addition, the HMI requirement promotes advance warning. This requirement is designed to prevent an overreaction by operators who need to respond to an emergency. By warning operators in advance when action is required, the operator is more likely to take appropriate action. The final requirement addressing situation awareness involves equalization of the workload. Essentially, the operator should be assisted more during high workload conditions and less during low workload conditions. To the extent the HMI design addresses the situation awareness requirements, operators are more likely to be alert and react properly when the system requires their attention.

Paragraph (c)(2) addresses another HMI issue, ''predictability and consistency'' in product behavior. For example, objects designed for predictability should move forward when an operator pushes the object or its controller forward, and valves designed for consistency should open in the same direction. In addition, new controls that require similar actions to older like controls should minimize the interference of learning in the transfer of knowledge and take advantage of already automated behaviors (*i.e.,* new controls should be ''backwards compatible''). The consistency envisioned by the HMI requirement would also apply to the terminology used for text and graphic displays.

Paragraph (c)(3) addresses a third HMI issue, which involves a human's limited memory and ability to process information. The fact that humans can process only one or two streams of information at a time without loss of information is termed ''selective attention.'' A remedy for selective attention is reducing an operator's information processing load by focusing on integrated information, the format of the information, and by testing decision aids to evaluate their true benefits. These solutions are in this paragraph. Finally, paragraph (c)(4) addresses miscellaneous human factor concerns that must be addressed at the design stage.

Paragraph (d) addresses design elements for on-board displays and controls. Paragraph (d)(1) articulates specific requirements for the location of displays and controls. These requirements need little explanation, since they are well-known principles. However, it must be recognized that these principles may at times conflict with each other. For example, it may not be possible to arrange controls according to their expected order of use and locate displays as close as possible to the controls that affect them. Trade-offs are often required in the design of effective, efficient and safe HMIs. System designers must ensure that appropriate personnel evaluate these critical decisions and make the appropriate trade-offs.

Paragraph (d)(2) pertains to information management by highlighting some of the industry recognized minimum standards for human-centered design of displays. Important information management issues include displaying information to emphasize its importance (*i.e.* alarms and other significant changes or unusual events presented with clear salient indicators, not by small changes or ambiguous displays that are easy to miss), avoiding unnecessary detail where text is used, avoiding text in all capital letters, and designing warnings to match the level of risk so that more dangerous conditions have aural and or visual signals that are associated with a higher level of urgency. Finally, paragraph (e) of the HMI appendix addresses requirements for problem management. These requirements essentially address in the design and implementation phase of development, the need to support situation awareness, response selection and contingency planning under unusual circumstances. These types of requirements are designed to avoid the errors humans tend to make during emergency situations and provide alternatives when the initial responses to the emergency fail.

Generally, all the literature concludes that as the nature of the task changes, performance related to those tasks inevitably changes. The nature and potential consequences of these changes can be determined by comparing the functions of an old system to that which is proposed in a new system. System evaluations of the impact of new technology on human operators must be conducted to help identify new sources of error. FRA believes that HMI evaluations conducted in accordance with the requirements of this appendix prior to implementation of new processor-based signal and train control technology will result in products that are safe and efficient.

IX. Regulatory Impact

A. Executive Order 12866 and DOT Regulatory Policies and Procedures

This final rule has been evaluated in accordance with existing policies and procedures and is considered ''significant'' under Executive Order 12866. It is also considered to be significant under DOT policies and procedures (*see* 44 FR 11034).

FRA has prepared a Final Regulatory Evaluation addressing the economic impact of the rule. This regulatory evaluation has been placed in the docket and is available for public inspection and copying during normal business hours at FRA's docket room at the Office of Chief Counsel, Federal Railroad Administration, 1120 Vermont Avenue, NW., Washington, DC 20590. Copies may also be obtained by submitting a written request to the FRA Docket Clerk at the above address.

B. Anticipated Costs and Benefits

Signal and train control systems act to prevent collisions between on-track equipment, in some cases to warn of defective track or other hazards and in some cases to govern train speed, preventing speed-related derailments. Thus the ultimate benefit of any signal and train control system's safety regulation is the provision of a safe operating environment for trains. The particular benefit of this rule is the facilitation of introducing new technology into the field of signal and train control under minimal government scrutiny.

The final rule regulates processor-based signal and train control systems. Technological advances have made these systems increasingly more attractive to railroads, yet existing FRA rules concerning design and testing of these systems impose restrictions which are unrealistic when applied to processor-based systems. In addition, in many instances, these systems are simply beyond the scope of current rules regulating traditional relay-based signal and train control systems. Consequently, FRA has been forced to regulate by exception, by issuing waivers or exemptions to its regulations on a case-by-case basis. This process has generally been recognized as time-consuming and unpredictable for the industry.

The performance standard presented here is that any new system must be at least as safe as the existing system. It does not mandate use of processor-based systems, but rather establishes performance standards for their design and use, should a railroad intend to implement one. FRA believes that a

railroad would adopt a new system under these rules only for one or more of the following three reasons:

(1) The new system is safer;

(2) The new system is less expensive and will not diminish the existing level of safety; or

(3) Continued maintenance of the existing system is no longer feasible.

In the first case, if a new system is safer, FRA assumes the railroad would adopt it only if it provided benefits which exceed costs to the railroad. Also, because the new system is safer, society at large would benefit. In the second case, if a new system were equally safe but less expensive, then the benefits would outweigh the costs to the railroad. Third, if the existing system is no longer feasible to maintain, the railroad under existing rules would be required to petition FRA in order to remove it, or would be required to replace it with a new system. FRA is not bound to grant such petitions, and the rule does not eliminate current rules regarding this abandonment process. In this instance, if the railroad replaces its system, FRA assumes it will choose the most cost-effective alternative, and the rule would ensure these alternatives are at least as safe as the current system. Only in this last case, where a railroad adopts a new system it would not otherwise have adopted, because its existing system has become impracticable to maintain, does FRA envision the rule could possibly impose a situation not in the railroad's best interest, and still one which imposes minimal costs on the railroad. FRA does not believe this case would be a common occurrence.

The final rule would require substantial safety documentation from the railroad. The documentation is required to explain how each railroad will comply with the performance standard. FRA expects these internal procedures to be more efficient than current FRA rules, since they will be particularized for each railroad.

An undetermined question is whether the cost of writing the railroad's safety plan and product safety plan exceeds the benefit from the increased flexibility. FRA does not believe so. It appears that the costliest part of the documentation will be the risk assessment. Currently, a substantial portion of this work is performed by suppliers. Each supplier now serving the rail industry uses some form of risk/safety analysis which can be documented, and although several suppliers commented that the documentation they currently gather is not adequate to meet the requirements of the rule, FRA believes that a much larger portion of the work required for the risk assessment has been done in standard engineering practices than suppliers' comments indicate. Nevertheless, FRA has added an additional means of compliance in the final rule, which will lessen any potential burden on suppliers.

The primary cost of this rule is the gathering of what FRA believes to be existing safety information into one source. This would likely be a single time expense for each system, unless the system were not to perform as expected in service. The corresponding benefit would be the railroad's ability to use the more flexible maintenance standards over the life of the system. An offset to the recurring benefit would be the cost of tracking failures which might lead to an unsafe condition.

Under the final rule, railroads using existing processor-based signal and train control systems would be required to maintain a software management control plan. FRA believes this is a desirable safety practice, as it would avoid incorrectly installing the wrong programming, either through hardware or software, in a system. FRA also believes that under the current regulations, replacing a processor or program would constitute disarrangement and would require physical testing of every device or appliance affected by that processor. In some cases, all of the switches and signals on a line are tied to a processor. It is costly and time consuming to conduct the currently required tests, and it is certainly less expensive to maintain a software management control plan, which is a step in avoiding a trigger for the disarrangement requirements. In new systems, which will include configuration management as part of the PSP, the maintenance plan may use configuration management to all but eliminate disarrangement issues. Further, configuration management will reduce the cost of troubleshooting by reducing the number of variables. Thus, insofar as existing processor-based systems are concerned, the rule will be less costly than the current rule, and FRA believes it will be more effective in promoting safety.

FRA has not quantified the above benefits because it has no way to estimate how many systems are likely to be covered by this rule, what the incremental costs will be, and when the benefits will occur. Because of the industry involvement in developing the NPRM (labor, management, and suppliers), FRA believes the benefits appear to outweigh the cost, since changes made to the NPRM language in order to derive the final rule were all likely to reduce potential burdens, without any decrease in safety. The rule does not appear to have any effect of transferring costs from the railroads to the suppliers. In addition, the suppliers as participants in the development of the NPRM, did not perceive that costs would be transferred to them.

In short, FRA does not know the magnitude of the benefits and costs because of the performance standard concepts embodied in the final rule, but believes that benefits will outweigh costs.

C. Regulatory Flexibility Act

The Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.*) requires a review of final rules to assess their impact on small entities, unless the Secretary certifies that a final rule will not have a significant economic impact on a substantial number of small entities. This final rule should not have a significant economic impact on small entities. The rule does not require the implementation of processor-based signal and train control systems, but merely sets forth a performance standard for the design and operation of them. Smaller entities are not required to develop new systems with costly risk analyses. In fact, the final rule has been designed to allow small entities to be able to ''recycle'' risk analyses by taking advantage of commercially-available products. Previously-developed risk analyses should require only minor changes to reflect how the product is to be used in the railroad's own operating environment. In conclusion, FRA believes that any impact on small entities will be minimal.

D. Paperwork Reduction Act

The information collection requirements in this final rule have been submitted for approval to the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501 *et seq.* The sections that contain the new information collection requirements and the estimated time to fulfill each requirement are as follows:

CFR section	Respondent universe	Total annual response	Average time per response	Total annual burden hours	Total annual burden cost
234.275—Processor—Based Systems—Deviations from Product Safety Plan (PSP)—Letters.	85 Railroads	25 letters	4 hours	100	$3,800
236.18—Software Management Control Plan	85 Railroads	45 plans	100 hours	4,500	297,000
236.905—Railroad Safety Program Plan (RSPP)	85 Railroads	15 plans	250 hours	3,750	153,000
—Response to FRA Request For Add'l Information.	85 Railroads	2 documents	8 hours	16	608
—FRA Approval of RSPP Modifications	85 Railroads	5 amendments	60 hours	300	13,080
236.907—Product Safety Plan (PSP)—Development	85 Railroads	30 plans	240 hours	7,200	900,000
236.909—Minimum Performance Standard—Petitions For Review and Approval.	85 Railroads	7 petitions	8 hours	56	3,696
—Performance of Full Risk Assessment	85 Railroads	5 assessments	3,000 hours	15,000	1,875,000
—Subsequent Years—Full Risk Assessment	85 Railroads	7 assessments	1,200 hours	8,400	1,050,000
—Abbreviated Risk Assessment	85 Railroads	25 assessments	240 hours	6,000	750,000
—Subsequent Years—Abbreviated Risk Assessment.	85 Railroads	10 assessments	60 hours	600	75,000
—Alternative Risk Assessment	25 assessments	5 assessments	3,000 hours	15,000	1,875,000
236.911—Exclusions—Notification to FRA	85 Railroads	20 notifications	80 hours	1,600	60,800
—Election to Have Excluded Products Covered By Submitting a Product Safety Plan (PSP).	85 Railroads	2 plans	240 hours	480	18,240
236.913—Notification/Submission to FRA of Joint Product Safety Plan.	85 Railroads	5 notices/plans	240 hours	1,200	45,600
—Petitions For Approval/Informational Filings	85 Railroads	32 petitions/filings	40 hours	1,280	48,640
—Responses to FRA Request For Further Info. After Informational Filing.	85 Railroads	20 documents	40 hours	800	30,400
—Responses to FRA Request For Further Info. After Agency Receipt of Notice of Product Development.	85 Railroads	20 documents	40 hours	800	30,400
—Technical Consultations Re: Notice of Product Dev.	85 Railroads	5 consultations	120 hours	600	75,000
—Petitions For Final Approval	85 Railroads	20 petitions	40 hours	800	30,400
—FRA Receipt of Petition & Request For More Info.	85 Railroads	10 documents	80 hours	800	30,400
—Agency Consultations To Decide on Petition	85 Railroads	10 consultations	40 hours	400	15,200
—Other Petitions For Approval	85 Railroads	5 petitions	60 hours	300	11,400
—FRA acknowledges receipt of petitions & Requests More Information.	85 Railroads	10 documents	40 hours	400	15,200
—Comments to FRA by Interested Parties	Public/RR Community	10 comments	8 hours	80	3,040
—Third Party Assessments of PSP	85 Railroads	3 assessments	4,000 hours	12,000	1,500,000
—Amendments to PSP	85 Railroads	15 amendments	40 hours	600	22,800
236.917—Retention of Records	85 Railroads	22 documents	40 hours	880	33,440
—Report of Inconsistencies with PSP to FRA	85 Railroads	40 reports	20 hours	800	30,400
236.919—Operations & Maintenance Manual	85 Railroads	30 manuals	120 hours	3,600	136,800
—Plans For Proper Maintenance, Repair, Inspection of Safety-Critical Products.	85 Railroads	30 plans	200 hours	6,000	228,000
—Hardware/Software/Firmware Revisions	85 Railroads	5 revisions	40 hours	200	7,600
—Identification of Safety-Critical Components	85 Railroads	10,000 markings	10 minutes	1,667	48,343
236.921—Training	85 Railroads	30 Training Prog	400 hours	12,000	456,000
—Training of Signalmen & Dispatchers	85 Railroads	220 sessions	40 hours/20 hours	8,400	1,050,000
236.923—Task Analysis/Basic Requirements—Rcds	85 Railroads	4,400 records	10 minutes	733	27,854

All estimates include the time for reviewing instructions; searching existing data sources; gathering or maintaining the needed data; and reviewing the information. For information or a copy of the paperwork package submitted to OMB contact Robert Brogan at 202–493–6292.

OMB is required to make a decision concerning the collection of information requirements contained in this final rule between 30 and 60 days after publication of this document in the **Federal Register**. Therefore, a comment to OMB is best assured of having its full effect if OMB receives it within 30 days of publication.

FRA cannot impose a penalty on persons for violating information collection requirements which do not display a current OMB control number, if required. FRA intends to obtain current OMB control numbers for any new information collection requirements resulting from this rulemaking action prior to the effective date of a final rule. The OMB control number, when assigned, will be announced by separate notice in the **Federal Register**.

E. Environmental Impact

FRA has evaluated this final regulation in accordance with the agency's ''Procedures for Considering Environmental Impacts'' as required by the National Environmental Policy Act (42 U.S.C. 4321 *et seq.*) and related statutes and directives. The agency has determined that the regulation would not have a significant impact on the human or natural environment and is categorically excluded from detailed environmental review pursuant to section 4(c)(20) of FRA's Procedures. Neither an environmental assessment or an environmental impact statement is required in this instance. The agency's review has confirmed the applicability of the categorical exclusion to this regulation and the conclusion that the final rule will not, when implemented, have a significant environmental impact.

F. Federalism Implications

This final rule has been analyzed in accordance with the principles and criteria contained in Executive Order 13132, and it has been determined that the rule does not have sufficient federalism implications to warrant the preparation of a federalism summary impact statement. FRA received no comments during the comment period concluding that federalism is impacted. FRA is therefore not required to include a federalism summary impact statement with the final rule. State and local

officials were involved in developing this rule. The RSAC has as permanent members two organizations representing State and local interests: the AASHTO and the ASRSM. RSAC regularly provides recommendations to the FRA Administrator for solutions to regulatory issues that reflect significant input from its State members.

G. Compliance With the Unfunded Mandates Reform Act of 1995

Pursuant to the Unfunded Mandates Reform Act of 1995 (Pub. L. 104–4) each Federal agency ''shall, unless otherwise prohibited by law, assess the effects of Federal Regulatory actions on State, local, and tribal governments, and the private sector (other than to the extent that such regulations incorporate requirements specifically set forth in law).'' Sec. 201. Section 202 of the Act further requires that ''before promulgating any general notice of proposed rulemaking that is likely to result in promulgation of any rule that includes any Federal mandate that may result in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any 1 year, and before promulgating any final rule for which a general notice of proposed rulemaking was published, the agency shall prepare a written statement * * *'' detailing the effect on State, local and tribal governments and the private sector. The rules issued today do not include any mandates which will result in the expenditure, in the aggregate, of $100,000,000 or more in any one year, and thus preparation of a statement is not required.

List of Subjects

49 CFR Part 209

Administrative practice and procedure.

49 CFR Part 234

Highway safety, Railroad safety.

49 CFR Part 236

Railroad safety, Reporting and recordkeeping requirements.

The Final Rule

■ In consideration of the foregoing, FRA amends chapter II, subtitle B, of title 49, Code of Federal Regulations as follows:

PART 209—[AMENDED]

■ 1. The authority citation for part 209 continues to read as follows:

Authority: 49 U.S.C. 20103, 20107, 20111, 20112, 20114; 28 U.S.C. 2461, note; and 49 CFR 1.49.

■ 2. Revise paragraph (a) of § 209.11 to read as follows:

§ 209.11 Request for confidential treatment.

(a) This section governs the procedures for requesting confidential treatment of any document filed with or otherwise provided to FRA in connection with its enforcement of statutes or FRA regulations related to railroad safety. For purposes of this section, ''enforcement'' shall include receipt of documents required to be submitted by FRA regulations, and all investigative and compliance activities, in addition to the development of violation reports and recommendations for prosecution.

* * * * *

PART 234—[AMENDED]

■ 3. The authority citation for part 234 continues to read as follows:

Authority: 49 U.S.C. 20103, 20107; 28 U.S.C. 2461, note; and 49 CFR 1.49.

■ 4. Add a new undesignated centerheading and new § 234.275 to read as follows:

Requirements for Processor-Based Systems

§ 234.275 Processor-based systems.

(a) The definitions in § 236.903 of this chapter shall apply to this section, where applicable.

(b) In lieu of compliance with the requirements of this subpart, a railroad may elect to qualify an existing product under part 236, subpart H of this chapter. Highway-rail grade crossing warning systems which contain new or novel technology or provide safety-critical data to a railroad signal system shall comply with part 236, subpart H of this chapter. New or novel technology refers to a technology not previously recognized for use as of March 7, 2005.

(c) The Product Safety Plan (see § 236.903 of this chapter) must explain how the performance objective sought to be addressed by each of the particular requirements of this subpart is met by the product, why the objective is not relevant to the product's design, or how safety requirements are satisfied using alternative means. Deviation from those particular requirements is authorized if an adequate explanation is provided, making reference to relevant elements of the Product Safety Plan, and if the product satisfies the performance standard set forth in § 236.909 of this chapter. (See § 236.907(a)(14) of this chapter.) Any existing products both used at highway-rail grade crossing warning systems and which provide safety-critical data to, or receive safety-critical data from, a railroad signal or train control system shall be included in the software management control plan as required in § 236.18 of this chapter.

(d) The following exclusions from the latitude provided by this section apply:

(1) Nothing in this section authorizes deviation from applicable design requirements for automated warning devices at highway-rail grade crossings in the Manual on Uniform Traffic Control Devices (MUTCD), 2000 Millennium Edition, Federal Highway Administration (FHWA), dated December 18, 2000, including Errata #1 to MUTCD 2000 Millennium Edition dated June 14, 2001 (*http://mutcd.fhwa.dot.gov/*).

(2) Nothing in this section authorizes deviation from the following requirements of this subpart:

(i) § 234.207(b) (Adjustment, repair, or replacement of a component);

(ii) § 234.209(b) (Interference with normal functioning of system);

(iii) § 234.211 (Security of warning system apparatus);

(iv) § 234.217 (Flashing light units);

(v) § 234.219 (Gate arm lights and light cable);

(vi) § 234.221 (Lamp voltage);

(vii) § 234.223 (Gate arm);

(viii) § 234.225 (Activation of warning system);

(ix) § 234.227 (Train detection apparatus)—if a train detection circuit is employed to determine the train's presence;

(x) § 234.229 (Shunting sensitivity)—if a conventional track circuit is employed;

(xi) § 234.231 (Fouling wires)—if a conventional train detection circuit is employed;

(xii) § 234.233 (Rail joints)—if a track circuit is employed;

(xiii) § 234.235 (Insulated rail joints)—if a track circuit is employed;

(xiv) § 234.237 (Reverse switch cut-out circuit); or

(xv) § 234.245 (Signs).

(e) Deviation from the requirement of § 234.203 (Control circuits) that circuits be designed on a fail-safe principle must be separately justified at the component, subsystem, and system level using the criteria of § 236.909 of this chapter.

■ 5. Amend Appendix A to part 234 by adding an entry for § 234.275 as follows:

APPENDIX A TO PART 234—SCHEDULE OF CIVIL PENALTIES

Section	Violation	Willful violation
* * * * *		
Subpart D—Maintenance, Inspection and Testing		
* * * * *		
234.275 Processor-Based Systems	$5,000	$7,500

PART 236—[AMENDED]

■ 6. Revise the authority citation for part 236 to read as follows:

Authority: 49 U.S.C. 20103, 20107, 20501—20505; 28 U.S.C. 2461, note; and 49 CFR 1.49.

■ 7. Amend § 236.0 to revise the section heading, paragraphs (a) and (b), and add new paragraphs (g) and (h) to read as follows:

§ 236.0 Applicability, minimum requirements, and penalties.

(a) Except as provided in paragraph (b) of this section, this part applies to all railroads.

(b) This part does not apply to—

(1) A railroad that operates only on track inside an installation that is not part of the general railroad system of transportation; or

(2) Rapid transit operations in an urban area that are not connected to the general railroad system of transportation.

* * * * *

(g) A person may also be subject to criminal penalties for knowingly and wilfully making a false entry in a record or report required to be made under this part, filing a false record or report, or violating any of the provisions of 49 U.S.C. 21311.

(h) The requirements of subpart H of this part apply to safety-critical processor-based signal and train control systems, including subsystems and components thereof, developed under the terms and conditions of that subpart.

■ 8. Add new § 236.18 to read as follows:

§ 236.18 Software management control plan.

(a) Within 6 months of June 6, 2005, each railroad shall develop and adopt a software management control plan for its signal and train control systems. A railroad commencing operations after June 6, 2005, shall adopt a software management control plan for its signal and train control systems prior to commencing operations.

(b) Within 30 months of the completion of the software management control plan, each railroad shall have fully implemented such plan.

(c) For purposes of this section, ''software management control plan'' means a plan designed to ensure that the proper and intended software version for each specific site and location is documented (mapped) and maintained through the life-cycle of the system. The plan must further describe how the proper software configuration is to be identified and confirmed in the event of replacement, modification, or disarrangement of any part of the system.

■ 9. Revise § 236.110 to read as follows:

§ 236.110 Results of tests.

(a) Results of tests made in compliance with §§ 236.102 to 236.109, inclusive; 236.376 to 236.387, inclusive; 236.576; 236.577; 236.586 to 236.589, inclusive; and 236.917(a) must be recorded on preprinted forms provided by the railroad or by electronic means, subject to approval by the FRA Associate Administrator for Safety. These records must show the name of the railroad, place and date, equipment tested, results of tests, repairs, replacements, adjustments made, and condition in which the apparatus was left. Each record must be:

(1) Signed by the employee making the test, or electronically coded or identified by number of the automated test equipment (where applicable);

(2) Unless otherwise noted, filed in the office of a supervisory official having jurisdiction; and

(3) Available for inspection and replication by FRA and FRA-certified State inspectors.

(b) Results of tests made in compliance with § 236.587 must be retained for 92 days.

(c) Results of tests made in compliance with § 236.917(a) must be retained as follows:

(1) Results of tests that pertain to installation or modification must be retained for the life-cycle of the equipment tested and may be kept in any office designated by the railroad; and

(2) Results of periodic tests required for maintenance or repair of the equipment tested must be retained until the next record is filed but in no case less than one year.

(d) Results of all other tests listed in this section must be retained until the next record is filed but in no case less than one year.

(e) Electronic or automated tracking systems used to meet the requirements contained in paragraph (a) of this section must be capable of being reviewed and monitored by FRA at any time to ensure the integrity of the system. FRA's Associate Administrator for Safety may prohibit or revoke a railroad's authority to utilize an electronic or automated tracking system in lieu of preprinted forms if FRA finds that the electronic or automated tracking system is not properly secured, is inaccessible to FRA, FRA-certified State inspectors, or railroad employees requiring access to discharge their assigned duties, or fails to adequately track and monitor the equipment. The Associate Administrator for Safety will provide the affected railroad with a written statement of the basis for his or her decision prohibiting or revoking the railroad from utilizing an electronic or automated tracking system.

■ 10. Add new § 236.787a to read as follows:

§ 236.787a Railroad.

Railroad means any form of non-highway ground transportation that runs on rails or electromagnetic guideways and any entity providing such transportation, including—

(a) Commuter or other short-haul railroad passenger service in a metropolitan or suburban area and commuter railroad service that was operated by the Consolidated Rail Corporation on January 1, 1979; and

(b) High speed ground transportation systems that connect metropolitan areas, without regard to whether those systems use new technologies not associated with traditional railroads; but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation.

■ 11. Add new subpart H to part 236 to read as follows:

Subpart H—Standards for Processor-Based Signal and Train Control Systems

Sec.

§ 236.901 Purpose and scope.

(a) What is the purpose of this subpart? The purpose of this subpart is to promote the safe operation of processor-based signal and train control systems, subsystems, and components that are safety-critical products, as defined in § 236.903, and to facilitate the development of those products.

(b) What topics does it cover? This subpart prescribes minimum, performance-based safety standards for safety-critical products, including requirements to ensure that the development, installation, implementation, inspection, testing, operation, maintenance, repair, and modification of those products will achieve and maintain an acceptable level of safety. This subpart also prescribes standards to ensure that personnel working with safety-critical products receive appropriate training. Each railroad may prescribe additional or more stringent rules, and other special instructions, that are not inconsistent with this subpart.

(c) What other rules apply? (1) This subpart does not exempt a railroad from compliance with the requirements of subparts A through G of this part, except to the extent a PSP explains to FRA Associate Administrator for Safety's satisfaction the following:

(i) How the objectives of any such requirements are met by the product;

(ii) Why the objectives of any such requirements are not relevant to the product; or

(iii) How the requirement is satisfied using alternative means. (See § 236.907(a)(14)).

(2) Products subject to this subpart are also subject to applicable requirements of parts 233, 234 and 235 of this chapter. See § 234.275 of this chapter with respect to use of this subpart to qualify certain products for use within highway-rail grade crossing warning systems.

(3) Information required to be submitted by this subpart that a submitter deems to be trade secrets, or commercial or financial information that is privileged or confidential under Exemption 4 of the Freedom of Information Act, 5 U.S.C. 552(b)(4), shall be so labeled in accordance with the provisions of § 209.11 of this chapter. FRA handles information so labeled in accordance with the provisions of § 209.11 of this chapter.

§ 236.903 Definitions.

As used in this subpart—

Associate Administrator for Safety means the Associate Administrator for Safety, FRA, or that person's delegate as designated in writing.

Component means an element, device, or appliance (including those whose nature is electrical, mechanical, hardware, or software) that is part of a system or subsystem.

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

Employer means a railroad, or contractor to a railroad, that directly engages or compensates individuals to perform the duties specified in § 236.921 (a).

Executive software means software common to all installations of a given product. It generally is used to schedule the execution of the site-specific application programs, run timers, read inputs, drive outputs, perform self-diagnostics, access and check memory, and monitor the execution of the application software to detect unsolicited changes in outputs.

FRA means the Federal Railroad Administration.

Full automatic operation means that mode of an automatic train control system capable of operating without external human influence, in which the locomotive engineer/operator may act as a passive system monitor, in addition to an active system controller.

Hazard means an existing or potential condition that can result in an accident.

High degree of confidence, as applied to the highest level of aggregation, means there exists credible safety analysis supporting the conclusion that the likelihood of the proposed condition associated with the new product being less safe than the previous condition is very small.

Human factors refers to a body of knowledge about human limitations, human abilities, and other human characteristics, such as behavior and motivation, that must be considered in product design.

Human-machine interface (HMI) means the interrelated set of controls and displays that allows humans to interact with the machine.

Initialization refers to the startup process when it is determined that a product has all required data input and the product is prepared to function as intended.

Mandatory directive has the meaning set forth in § 220.5 of this chapter.

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

Mean Time To Hazardous Event (MTTHE) means the average or expected time that a subsystem or component will operate prior to the occurrence of an unsafe failure.

New or next-generation train control system means a train control system using technologies not in use in revenue service at the time of PSP submission or without established histories of safe practice.

Petition for approval means a petition to FRA for approval to use a product on a railroad as described in its PSP. The petition for approval is to contain information that is relevant to determining the safety of the resulting system; relevant to determining compliance with this part; and relevant to determining the safety of the product, including a complete copy of the product's PSP and supporting safety analysis.

Predefined change means any post-implementation modification to the use of a product that is provided for in the PSP (see § 236.907(b)).

Previous Condition refers to the estimated risk inherent in the portion of the existing method of operation that is relevant to the change under analysis (including the elements of any existing signal or train control system relevant to the review of the product).

Processor-based, as used in this subpart, means dependent on a digital processor for its proper functioning.

Product means a processor-based signal or train control system, subsystem, or component.

Product Safety Plan (or *PSP*) refers to a formal document which describes in detail all of the safety aspects of the product, including but not limited to procedures for its development, installation, implementation, operation, maintenance, repair, inspection, testing and modification, as well as analyses supporting its safety claims, as described in § 236.907.

Railroad Safety Program Plan (or *RSPP*) refers to a formal document which describes a railroad's strategy for addressing safety hazards associated with operation of products under this subpart and its program for execution of such strategy though the use of PSP requirements, as described in § 236.905.

Revision control means a chain of custody regimen designed to positively identify safety-critical components and spare equipment availability, including repair/replacement tracking in accordance with procedures outlined in the PSP.

Risk means the expected probability of occurrence for an individual accident

event (probability) multiplied by the severity of the expected consequences associated with the accident (severity).

Risk assessment means the process of determining, either quantitatively or qualitatively, the measure of risk associated with use of the product under all intended operating conditions or the previous condition.

Safety-critical, as applied to a function, a system, or any portion thereof, means the correct performance of which is essential to safety of personnel or equipment, or both; or the incorrect performance of which could cause a hazardous condition, or allow a hazardous condition which was intended to be prevented by the function or system to exist.

Subsystem means a defined portion of a system.

System refers to a signal or train control system and includes all subsystems and components thereof, as the context requires.

System Safety Precedence means the order of precedence in which methods used to eliminate or control identified hazards within a system are implemented.

Validation means the process of determining whether a product's design requirements fulfill its intended design objectives during its development and life-cycle. The goal of the validation process is to determine ''whether the correct product was built.''

Verification means the process of determining whether the results of a given phase of the development cycle fulfill the validated requirements established at the start of that phase. The goal of the verification process is to determine ''whether the product was built correctly.''

§ 236.905 Railroad Safety Program Plan (RSPP).

(a) *What is the purpose of an RSPP?* A railroad subject to this subpart shall develop an RSPP, subject to FRA approval, that serves as its principal safety document for all safety-critical products. The RSPP must establish the minimum PSP requirements that will govern the development and implementation of all products subject to this subpart, consistent with the provisions contained in § 236.907.

(b) *What subject areas must the RSPP address?* The railroad's RSPP must address, at a minimum, the following subject areas:

(1) *Requirements and concepts.* The RSPP must require a description of the preliminary safety analysis, including:

(i) A complete description of methods used to evaluate a system's behavioral characteristics;

(ii) A complete description of risk assessment procedures;

(iii) The system safety precedence followed; and

(iv) The identification of the safety assessment process.

(2) *Design for verification and validation.* The RSPP must require the identification of verification and validation methods for the preliminary safety analysis, initial development process, and future incremental changes, including standards to be used in the verification and validation process, consistent with Appendix C to this part. The RSPP must require that references to any non-published standards be included in the PSP.

(3) *Design for human factors.* The RSPP must require a description of the process used during product development to identify human factors issues and develop design requirements which address those issues.

(4) *Configuration management control plan.* The RSPP must specify requirements for configuration management for all products to which this subpart applies.

(c) *How are RSPP's approved?* (1) Each railroad shall submit a petition for approval of an RSPP in triplicate to the Associate Administrator for Safety, FRA, 1120 Vermont Avenue, NW., Mail Stop 25, Washington, DC 20590. The petition must contain a copy of the proposed RSPP, and the name, title, address, and telephone number of the railroad's primary contact person for review of the petition.

(2) Normally within 180 days of receipt of a petition for approval of an RSPP, FRA:

(i) Grants the petition, if FRA finds that the petition complies with applicable requirements of this subpart, attaching any special conditions to the approval of the petition as necessary to carry out the requirements of this subpart;

(ii) Denies the petition, setting forth reasons for denial; or

(iii) Requests additional information.

(3) If no action is taken on the petition within 180 days, the petition remains pending for decision. The petitioner is encouraged to contact FRA for information concerning its status.

(4) FRA may reopen consideration of any previously-approved petition for cause, providing reasons for such action.

(d) *How are RSPP's modified?* (1) Railroads shall obtain FRA approval for any modification to their RSPP which affects a safety-critical requirement of a PSP. Other modifications do not require FRA approval.

(2) Petitions for FRA approval of RSPP modifications are subject to the same procedures as petitions for initial RSPP approval, as specified in paragraph (c) of this section. In addition, such petitions must identify the proposed modification(s) to be made, the reason for the modification(s), and the effect of the modification(s) on safety.

§ 236.907 Product Safety Plan (PSP).

(a) *What must a PSP contain?* The PSP must include the following:

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

(2) A description of the railroad operation or categories of operations on which the product is designed to be used, including train movement density, gross tonnage, passenger train movement density, hazardous materials volume, railroad operating rules, and operating speeds;

(3) An operational concepts document, including a complete description of the product functionality and information flows;

(4) A safety requirements document, including a list with complete descriptions of all functions which the product performs to enhance or preserve safety;

(5) A document describing the manner in which product architecture satisfies safety requirements;

(6) A hazard log consisting of a comprehensive description of all safety-relevant hazards to be addressed during the life cycle of the product, including maximum threshold limits for each hazard (for unidentified hazards, the threshold shall be exceeded at one occurrence);

(7) A risk assessment, as prescribed in § 236.909 and Appendix B to this part;

(8) A hazard mitigation analysis, including a complete and comprehensive description of all hazards to be addressed in the system design and development, mitigation techniques used, and system safety precedence followed, as prescribed by the applicable RSPP;

(9) A complete description of the safety assessment and verification and validation processes applied to the product and the results of these processes, describing how subject areas covered in Appendix C to this part are either: addressed directly, addressed using other safety criteria, or not applicable;

(10) A complete description of the safety assurance concepts used in the product design, including an

explanation of the design principles and assumptions;

(11) A human factors analysis, including a complete description of all human-machine interfaces, a complete description of all functions performed by humans in connection with the product to enhance or preserve safety, and an analysis in accordance with Appendix E to this part or in accordance with other criteria if demonstrated to the satisfaction of the Associate Administrator for Safety to be equally suitable;

(12) A complete description of the specific training of railroad and contractor employees and supervisors necessary to ensure the safe and proper installation, implementation, operation, maintenance, repair, inspection, testing, and modification of the product;

(13) 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 product. These procedures, including calibration requirements, shall be consistent with or explain deviations from the equipment manufacturer's recommendations;

(14) An analysis of the applicability of the requirements of subparts A through G of this part to the product that may no longer apply or are satisfied by the product using an alternative method, and a complete explanation of the manner in which those requirements are otherwise fulfilled (see § 234.275 of this chapter and § 236.901(c));

(15) A complete description of the necessary security measures for the product over its life-cycle;

(16) A complete description of each warning to be placed in the Operations and Maintenance Manual identified in § 236.919, and of all warning labels required to be placed on equipment as necessary to ensure safety;

(17) 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;

(18) A complete description of:

(i) 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 (repair, replacement, adjustment) is performed; and

(ii) Each record necessary to ensure the safety of the system that is associated with periodic maintenance, inspections, tests, repairs, replacements, adjustments, and the system's resulting conditions, including records of component failures resulting in safety-relevant hazards (see § 236.917(e)(3));

(19) A complete description of any safety-critical assumptions regarding availability of the product, and a complete description of all backup methods of operation; and

(20) A complete description of all incremental and predefined changes (see paragraphs (b) and (c) of this section).

(b) *What requirements apply to predefined changes?* (1) Predefined changes are not considered design modifications requiring an entirely new safety verification process, a revised PSP, and an informational filing or petition for approval in accordance with § 236.915. However, the risk assessment for the product must demonstrate that operation of the product, as modified by any predefined change, satisfies the minimum performance standard.

(2) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change. (Software changes involving safety functional requirements or safety critical hazard mitigation processes for components in use are also addressed in paragraph (c) of this section.)

(c) *What requirements apply to other product changes?* (1) Incremental changes are planned product version changes described in the initial PSP where slightly different specifications are used to allow the gradual enhancement of the product's capabilities. Incremental changes shall require verification and validation to the extent the changes involve safety-critical functions.

(2) Changes classified as maintenance require validation.

(d) *What are the responsibilities of the railroad and product supplier regarding communication of hazards?* (1) The PSP shall specify all contractual arrangements with hardware and software suppliers for immediate notification of any and all safety critical software upgrades, patches, or revisions for their processor-based system, sub-system, or component, and the reasons for such changes from the suppliers, whether or not the railroad has experienced a failure of that safety-critical system, sub-system, or component.

(2) The PSP shall specify the railroad's procedures for action upon notification of a safety-critical upgrade, patch, or revision for this processor-based system, sub-system, or component, and until the upgrade, patch, or revision has been installed; and such action shall be consistent with the criterion set forth in § 236.915(d) as if the failure had occurred on that railroad.

(3) The PSP must identify configuration/revision control measures designed to ensure that safety-functional requirements and safety-critical hazard mitigation processes are not compromised as a result of any such change, and that any such change can be audited.

(4) Product suppliers entering into contractual arrangements for product support described in a PSP must promptly report any safety-relevant failures and previously unidentified hazards to each railroad using the product.

§ 236.909 Minimum performance standard.

(a) *What is the minimum performance standard for products covered by this subpart?* The safety analysis included in the railroad's PSP must establish with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. The railroad shall determine, prior to filing its petition for approval or informational filing, that this standard has been met and shall make available the necessary analyses and documentation as provided in this subpart.

(b) *How does FRA determine whether the PSP requirements for products covered by subpart H have been met?* With respect to any FRA review of a PSP, the Associate Administrator for Safety independently determines whether the railroad's safety case establishes with a high degree of confidence that introduction of the product will not result in risk that exceeds the previous condition. In evaluating the sufficiency of the railroad's case for the product, the Associate Administrator for Safety considers, as applicable, the factors pertinent to evaluation of risk assessments, listed in § 236.913(g)(2).

(c) *What is the scope of a full risk assessment required by this section?* A full risk assessment performed under this subpart must address the safety risks affected by the introduction, modification, replacement, or enhancement of a product. This includes risks associated with the previous condition which are no longer present as a result of the change, new risks not present in the previous condition, and risks neither newly created nor eliminated whose nature

(probability of occurrence or severity) is nonetheless affected by the change.

(d) *What is an abbreviated risk assessment, and when may it be used?* (1) An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard if:

(i) No new hazards are introduced as a result of the change;

(ii) Severity of each hazard associated with the previous condition does not increase from the previous condition; and

(iii) Exposure to such hazards does not change from the previous condition.

(2) An abbreviated risk assessment supports the finding required by paragraph (a) of this section if it establishes that the resulting MTTHE for the proposed product is greater than or equal to the MTTHE for the system, component or method performing the same function in the previous condition. This determination must be supported by credible safety analysis sufficient to persuade the Associate Administrator for Safety that the likelihood of the new product's MTTHE being less than the MTTHE for the system, component, or method performing the same function in the previous condition is very small.

(3) Alternatively, an abbreviated risk assessment supports the finding required by paragraph (a) of this section if:

(i) The probability of failure for each hazard of the product is equal to or less the corresponding recommended Specific Quantitative Hazard Probability Ratings classified as more favorable than ''undesirable'' by AREMA Manual Part 17.3.5 (Recommended Procedure for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications), or—in the case of a hazard classified as undesirable—the Associate Administrator for Safety concurs that mitigation of the hazard within the framework of the electronic system is not practical and the railroad proposes reasonable steps to undertake other mitigation. The Director of the Federal Register approves the incorporation by reference of the entire AREMA Communications and Signal Manual, Volume 4, Section 17—Quality Principles (2005) in this section in accordance with 5 U.S.C. 552(a) and 1 CFR part 51. You may obtain a copy of the incorporated standard from American Railway Engineering and Maintenance of Way Association, 8201 Corporation Drive, Suite 1125, Landover, MD 20785–2230. You may inspect a copy of the incorporated standard at the Federal Railroad Administration, Docket Clerk, 1120 Vermont Ave., NW., Suite 7000, or at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, call 202–741–6030, or go to *http://www.archives.gov/federal_register/code_of_federal_regulations/ibr_locations.html*;

(ii) The product is developed in accordance with:

(A) AREMA Manual Part 17.3.1 (Communications and Signal Manual of Recommended Practices, Recommended Safety Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications);

(B) AREMA Manual Part 17.3.3 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hardware Analysis for Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications);

(C) AREMA Manual Part 17.3.5 (Communications and Signal Manual of Recommended Practices, Recommended Practice for Hazard Identification and Management of Vital Electronic/Software-Based Equipment Used in Signal and Train Control Applications);

(D) Appendix C of this subpart; and

(iii) Analysis supporting the PSP suggests no credible reason for believing that the product will be less safe than the previous condition.

(e) *How are safety and risk measured for the full risk assessment?* Risk assessment techniques, including both qualitative and quantitative methods, are recognized as providing credible and useful results for purposes of this section if they apply the following principles:

(1) Safety levels must be measured using competent risk assessment methods and must be expressed as the total residual risk in the system over its expected life-cycle after implementation of all mitigating measures described in the PSP. Appendix B to this part provides criteria for acceptable risk assessment methods. Other methods may be acceptable if demonstrated to the satisfaction of the Associate Administrator for Safety to be equally suitable.

(2) For the previous condition and for the life-cycle of the product, risk levels must be expressed in units of consequences per unit of exposure.

(i) In all cases exposure must be expressed as total train miles traveled per year. 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. A railroad may, as an alternative, use a risk metric in which consequences are measured strictly in terms of fatalities.

(ii) In those cases where there is passenger traffic, a second risk metric must be calculated, using passenger-miles traveled per year as the exposure, and total societal costs of passenger injuries and fatalities, resulting from preventable accidents associated with the function(s) performed by the system, as the consequences.

(3) If the description of railroad operations for the product required by § 236.907(a)(2) involves changes to the physical or operating conditions on the railroad prior to or within the expected life cycle of the product subject to review under this subpart, the previous condition shall be adjusted to reflect the lower risk associated with systems needed to maintain safety and performance at higher speeds or traffic volumes. In particular, the previous condition must be adjusted for assumed implementation of systems necessary to support higher train speeds as specified in § 236.0, as well as other changes required to support projected increases in train operations. The following specific requirements apply:

(i) If the current method of operation would not be adequate under § 236.0 for the proposed operations, then the adjusted previous condition must include a system as required under § 236.0, applied as follows:

(A) The minimum system where a passenger train is operated at a speed of 60 or more miles per hour, or a freight train is operated at a speed of 50 or more miles per hour, shall be a traffic control system;

(B) The minimum system where a train is operated at a speed of 80 or more miles per hour, but not more than 110 miles per hour, shall be an automatic cab signal system with automatic train control; and

(C) The minimum system where a train is operated at a speed of more than 110 miles per hour shall be a system determined by the Associate Administrator for Safety to provide an equivalent level of safety to systems required or authorized by FRA for comparable operations.

(ii) If the current method of operation would be adequate under § 236.0 for the proposed operations, but the current system is not at least as safe as a traffic control system, then the adjusted previous condition must include a traffic control system in the event of any change that results in:

(A) An annual average daily train density of more than twelve trains per day; or

(B) An increase in the annual average daily density of passenger trains of more than four trains per day.

(iii) Paragraph (e)(3)(ii)(A) of this section shall apply in all situations where train volume will exceed more than 20 trains per day but shall not apply to situations where train volume will exceed 12 trains per day but not exceed 20 trains per day, if in its PSP the railroad makes a showing sufficient to establish, in the judgment of the Associate Administrator for Safety, that the current method of operation is adequate for a specified volume of traffic in excess of 12 trains per day, but not more than 20 trains per day, without material delay in the movement of trains over the territory and without unreasonable expenditures to expedite those movements when compared with the expense of installing and maintaining a traffic control system.

(4) In the case review of a PSP that has been consolidated with a proceeding pursuant to part 235 of this subchapter (see § 236.911(b)), the base case shall be determined as follows:

(i) If FRA determines that discontinuance or modification of the system should be granted without regard to whether the product is installed on the territory, then the base case shall be the conditions that would obtain on the territory following the discontinuance or modification. **Note:** This is an instance in which the base case is posited as greater risk than the actual (unadjusted) previous condition because the railroad would have obtained relief from the requirement to maintain the existing signal or train control system even if no new product had been proffered.

(ii) If FRA determines that discontinuance or modification of the system should be denied without regard to whether the product is installed on the territory, then the base case shall remain the previous condition (unadjusted).

(iii) If, after consideration of the application and review of the PSP, FRA determines that neither paragraph (e)(4)(i) nor paragraph (e)(4)(ii) of this section should apply, FRA will establish a base case that is consistent with safety and in the public interest.

§ 236.911 Exclusions.

(a) *Does this subpart apply to existing systems?* The requirements of this subpart do not apply to products in service as of June 6, 2005. Railroads may continue to implement and use these products and components from these existing products.

(b) *How will transition cases be handled?* Products designed in accordance with subparts A through G of this part which are not in service but are developed or are in the developmental stage prior to March 7, 2005, may be excluded upon notification to FRA by June 6, 2005, if placed in service by March 7, 2008. Railroads may continue to implement and use these products and components from these existing products. A railroad may at any time elect to have products that are excluded made subject to this subpart by submitting a PSP as prescribed in § 236.913 and otherwise complying with this subpart.

(c) *How are office systems handled?* The requirements of this subpart do not apply to existing office systems and future deployments of existing office system technology. However, a subsystem or component of an office system must comply with the requirements of this subpart if it performs safety-critical functions within, or affects the safety performance of, a new or next-generation train control system. For purposes of this section, ''office system'' means a centralized computer-aided train-dispatching system or centralized traffic control board.

(d) *How are modifications to excluded products handled?* Changes or modifications to products otherwise excluded from the requirements of this subpart by this section are not excluded from the requirements of this subpart if they result in a degradation of safety or a material increase in safety-critical functionality.

(e) *What other rules apply to excluded products?* Products excluded by this section from the requirements of this subpart remain subject to subparts A through G of this part as applicable.

§ 236.913 Filing and approval of PSPs.

(a) *Under what circumstances must a PSP be prepared?* A PSP must be prepared for each product covered by this subpart. A joint PSP must be prepared when:

(1) The territory on which a product covered by this subpart is normally subject to joint operations, or is operated upon by more than one railroad; and

(2) The PSP involves a change in method of operation.

(b) *Under what circumstances must a railroad submit a petition for approval for a PSP or PSP amendment, and when may a railroad submit an informational filing?* Depending on the nature of the proposed product or change, the railroad shall submit either an informational filing or a petition for approval. Submission of a petition for approval is required for PSPs or PSP amendments concerning installation of new or next-generation train control systems. All other actions that result in the creation of a PSP or PSP amendment require an informational filing and are handled according to the procedures outlined in paragraph (c) of this section. Applications for discontinuance and material modification of signal and train control systems remain governed by parts 235 and 211 of this chapter; and petitions subject to this section may be consolidated with any relevant application for administrative handling.

(c) *What are the procedures for informational filings?* The following procedures apply to PSPs and PSP amendments which do not require submission of a petition for approval, but rather require an informational filing:

(1) Not less than 180 days prior to planned use of the product in revenue service as described in the PSP or PSP amendment, the railroad shall submit an informational filing to the Associate Administrator for Safety, FRA, 1120 Vermont Avenue, NW., Mail Stop 25, Washington, DC 20590. The informational filing must provide a summary description of the PSP or PSP amendment, including the intended use of the product, and specify the location where the documentation as described in § 236.917(e)(1) is maintained.

(2) Within 60 days of receipt of the informational filing, FRA:

(i) Acknowledges receipt of the filing;

(ii) Acknowledges receipt of the informational filing and requests further information; or

(iii) Acknowledges receipt of the filing and notifies the railroad, for good cause, that the filing will be considered as a petition for approval as set forth in paragraph (d) of this section, and requests such further information as may be required to initiate action on the petition for approval. Examples of good cause, any one of which is sufficient, include: the PSP describes a product with unique architectural concepts; the PSP describes a product that uses design or safety assurance concepts considered outside existing accepted practices (see Appendix C); and the PSP describes a locomotive-borne product that commingles safety-critical train control processing functions with locomotive operational functions. In addition, good cause includes any instance where the PSP or PSP amendment does not appear to support its safety claim of satisfaction of the performance standard, after FRA has requested further information as

provided in paragraph (c)(2)(ii) of this section.

(d) *What procedures apply to petitions for approval?* The following procedures apply to PSPs and PSP amendments which require submission of a petition for approval:

(1) *Petitions for approval involving prior FRA consultation.*

(i) The railroad may file a Notice of Product Development with the Associate Administrator for Safety not less than 30 days prior to the end of the system design review phase of product development and 180 days prior to planned implementation, inviting FRA to participate in the design review process and receive periodic briefings and updates as needed to follow the course of product development. At a minimum, the Notice of Product Development must contain a summary description of the product to be developed and a brief description of goals for improved safety.

(ii) Within 15 days of receipt of the Notice of Product Development, the Associate Administrator for Safety either acknowledges receipt or acknowledges receipt and requests more information.

(iii) If FRA concludes that the Notice of Product Development contains sufficient information, the Associate Administrator for Safety determines the extent and nature of the assessment and review necessary for final product approval. FRA may convene a technical consultation as necessary to discuss issues related to the design and planned development of the product.

(iv) Within 60 days of receiving the Notice of Product Development, the Associate Administrator for Safety provides a letter of preliminary review with detailed findings, including whether the design concepts of the proposed product comply with the requirements of this subpart, whether design modifications are necessary to meet the requirements of this subpart, and the extent and nature of the safety analysis necessary to comply with this subpart.

(v) Not less than 60 days prior to use of the product in revenue service, the railroad shall file with the Associate Administrator for Safety a petition for final approval.

(vi) Within 30 days of receipt of the petition for final approval, the Associate Administrator for Safety either acknowledges receipt or acknowledges receipt and requests more information. Whenever possible, FRA acts on the petition for final approval within 60 days of its filing by either granting it or denying it. If FRA neither grants nor denies the petition for approval within 60 days, FRA advises the petitioner of the projected time for decision and conducts any further consultations or inquiries necessary to decide the matter.

(2) *Other petitions for approval.* The following procedures apply to petitions for approval of PSPs which do not involve prior FRA consultation as described in paragraph (d)(1) of this section.

(i) Not less than 180 days prior to use of a product in revenue service, the railroad shall file with the Associate Administrator for Safety a petition for approval.

(ii) Within 60 days of receipt of the petition for approval, FRA either acknowledges receipt, or acknowledges receipt and requests more information.

(iii) Whenever possible, considering the scope, complexity, and novelty of the product or change, FRA acts on the petition for approval within 180 days of its filing by either granting it or denying it. If FRA neither grants nor denies the petition for approval within 180 days, it remains pending, and FRA provides the petitioner with a statement of reasons why the petition has not yet been approved.

(e) *What role do product users play in the process of safety review?* (1) FRA will publish in the **Federal Register** periodically a topic list including docket numbers for informational filings and a petition summary including docket numbers for petitions for approval.

(2) Interested parties may submit to FRA information and views pertinent to FRA's consideration of an informational filing or petition for approval. FRA considers comments to the extent practicable within the periods set forth in this section. In a proceeding consolidated with a proceeding under part 235 of this chapter, FRA considers all comments received.

(f) *Is it necessary to complete field testing prior to filing the petition for approval?* A railroad may file a petition for approval prior to completion of field testing of the product. The petition for approval should additionally include information sufficient for FRA to arrange monitoring of the tests. The Associate Administrator for Safety may approve a petition for approval contingent upon successful completion of the test program contained in the PSP or hold the petition for approval pending completion of the tests.

(g) *How are PSPs approved?* (1) The Associate Administrator for Safety grants approval of a PSP when:

(i) The petition for approval has been properly filed and contains the information required in § 236.907;

(ii) FRA has determined that the PSP complies with the railroad's approved RSPP and applicable requirements of this subpart; and

(iii) The risk assessment supporting the PSP demonstrates that the proposed product satisfies the minimum performance standard stated in § 236.909.

(2) The Associate Administrator for Safety considers the following applicable factors when evaluating the risk assessment:

(i) The extent to which recognized standards have been utilized in product design and in the relevant safety analysis;

(ii) The availability of quantitative data, including calculations of statistical confidence levels using accepted methods, associated with risk estimates;

(iii) The complexity of the product and the extent to which it will incorporate or deviate from design practices associated with previously established histories of safe operation;

(iv) The degree of rigor and precision associated with the safety analyses, including the comprehensiveness of the qualitative analyses, and the extent to which any quantitative results realistically reflect appropriate sensitivity cases;

(v) The extent to which validation of the product has included experiments and tests to identify uncovered faults in the operation of the product;

(vi) The extent to which identified faults are effectively addressed;

(vii) Whether the risk assessment for the previous condition was conducted using the same methodology as that for operation under the proposed condition; and

(viii) If an independent third-party assessment is required or is performed at the election of the supplier or railroad, the extent to which the results of the assessment are favorable.

(3) The Associate Administrator for Safety also considers when assessing PSPs the safety requirements for the product within the context of the proposed method of operations, including:

(i) The degree to which the product is relied upon as the primary safety system for train operations; and

(ii) The degree to which the product is overlaid upon and its operation is demonstrated to be independent of safety-relevant rules, practices and systems that will remain in place following the change under review.

(4) As necessary to ensure compliance with this subpart and with the RSPP, FRA may attach special conditions to the approval of the petition.

(5) Following the approval of a petition, FRA may reopen consideration of the petition for cause. Cause for reopening a petition includes such circumstances as a credible allegation of error or fraud, assumptions determined to be invalid as a result of in-service experience, or one or more unsafe events calling into question the safety analysis underlying the approval.

(h) *Under what circumstances may a third-party assessment be required, and by whom may it be conducted?* (1) The PSP must be supported by an independent third party assessment of the product when FRA concludes it is necessary based upon consideration of the following factors:

(i) Those factors listed in paragraphs (g)(2)(i) through (g)(2)(vii) of this section;

(ii) The sufficiency of the assessment or audit previously conducted at the election of a supplier or railroad; and

(iii) Whether applicable requirements of subparts A through G of this part are satisfied.

(2) 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 supplier of the product. An entity that is owned or controlled by the supplier, that is under common ownership or control with the supplier, or that is otherwise involved in the development of the product is not considered ''independent'' within the meaning of this section. FRA may maintain a roster of recognized technically competent entities as a service to railroads selecting reviewers under this section; however, a railroad is not limited to entities currently listed on any such roster.

(3) The third-party assessment must, at a minimum, consist of the activities and result in production of documentation meeting the requirements of Appendix D to this part. However, when requiring an assessment pursuant to this section, FRA specifies any requirements in Appendix D to this part which the agency has determined are not relevant to its concerns and, therefore, need not be included in the assessment. The railroad shall make the final assessment report available to FRA upon request.

(i) *How may a PSP be amended?* A railroad may submit an amendment to a PSP at any time in the same manner as the initial PSP. Notwithstanding the otherwise applicable requirements found in this section and § 236.915, changes affecting the safety-critical functionality of a product may be made prior to the submission and approval of the PSP amendment as necessary in order to mitigate risk.

(j) *How may field testing be conducted prior to PSP approval?* (1) Field testing of a product may be conducted prior to the approval of a PSP by the submission of an informational filing by a railroad. The FRA will arrange to monitor the tests based on the information provided in the filing, which must include:

(i) A complete description of the product;

(ii) An operational concepts document;

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

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

(v) The date testing will begin;

(vi) The location of the testing; and

(vii) A description of any effect the testing will have on the current method of operation.

(2) FRA may impose such additional conditions on this testing as may be necessary for the safety of train operations. Exemptions from regulations other than those contained in this part must be requested through waiver procedures in part 211 of this chapter.

§ 236.915 Implementation and operation.

(a) *When may a product be placed or retained in service?* (1) Except as stated in paragraphs (a)(2) and (a)(3) of this section, a railroad may operate in revenue service any product 180 days after filing with FRA the informational filing for that product. The FRA filing date can be found in FRA's acknowledgment letter referred to in § 236.913(c)(2).

(2) Except as stated in paragraph (a)(3) of this section, if FRA approval is required for a product, the railroad shall not operate the product in revenue service until after the Associate Administrator for Safety has approved the petition for approval for that product pursuant to § 236.913.

(3) If after product implementation FRA elects, for cause, to treat the informational filing for the product as a petition for approval, the product may remain in use if otherwise consistent with the applicable law and regulations. FRA may impose special conditions for use of the product during the period of review for cause.

(b) *How does the PSP relate to operation of the product?* Each railroad shall comply with all provisions in the PSP for each product it uses and shall operate within the scope of initial operational assumptions and predefined changes identified by the PSP. Railroads may at any time submit an amended PSP according to the procedures outlined in § 236.913.

(c) *What precautions must be taken prior to interference with the normal functioning of a product?* The normal functioning of any safety-critical product must not be interfered with in testing or otherwise without first taking measures to provide for safe movement of trains, locomotives, roadway workers and on-track equipment that depend on normal functioning of such product.

(d) *What actions must be taken immediately upon failure of a safety-critical component?* When any safety-critical product 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 are completed, a railroad shall take appropriate action as specified in the PSP. See also §§ 236.907(d), 236.917(b).

§ 236.917 Retention of records.

(a) *What life-cycle and maintenance records must be maintained?* (1) The railroad shall maintain at a designated office on the railroad:

(i) For the life-cycle of the product, adequate documentation to demonstrate that the PSP meets the safety requirements of the railroad's RSPP and applicable standards in this subpart, including the risk assessment; and

(ii) An Operations and Maintenance Manual, pursuant to § 236.919; and

(iii) Training records pursuant to § 236.923(b).

(2) Results of inspections and tests specified in the PSP must be recorded as prescribed in § 236.110.

(3) Contractors of the railroad shall maintain at a designated office training records pursuant to § 236.923(b).

(b) *What actions must the railroad take in the event of occurrence of a safety-relevant hazard?* After the product is placed in service, the railroad shall maintain a database of all safety-relevant hazards as set forth in the PSP and those that had not been previously identified in the PSP. If the frequency of the safety-relevant hazards exceeds the threshold set forth in the PSP (see § 236.907(a)(6)), 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, 1120 Vermont Ave., NW., 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 the safety-relevant hazard(s) below the threshold set forth in the PSP; and

(3) Provide a final report 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 PSP when the problem is resolved.

§ 236.919 Operations and Maintenance Manual.

(a) The railroad shall catalog and maintain all documents as specified in the PSP for the installation, maintenance, repair, modification, inspection, and testing of the product 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 products must be adequate in detail and must be made available for inspection by FRA and FRA-certified State inspectors where such products 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 PSP.

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

§ 236.921 Training and qualification program, general.

(a) *When is training necessary and who must be trained?* Employers shall establish and implement training and qualification programs for products subject to this subpart. These programs must meet the minimum requirements set forth in the PSP and in §§ 236.923 through 236.929 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 products, 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) *What competencies are required?* 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 processor-based signal and train control equipment.

§ 236.923 Task analysis and basic requirements.

(a) *How must training be structured and delivered?* As part of the program required by § 236.921, 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 products. 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 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 § 236.921(a) to successfully complete a training curriculum and pass an examination that covers the product 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 at intervals specified in the PSP 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 § 236.923(a)(1) verifying the adequacy of the training material and its validity with respect to current railroads products and operations.

(b) *What training records are required?* 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.

§ 236.925 Training specific to control office personnel.

Any person responsible for issuing or communicating mandatory directives in territory where products are or will be in use must be trained in the following areas, as applicable:

(a) 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;

(b) 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

(c) 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.

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

(a) *What elements apply to 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 must be defined in the PSP and the following elements must 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 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) *How must locomotive engineer training be conducted?* Training required under this subpart for a locomotive engineer, together with required records, must be integrated into the program of training required by part 240 of this chapter.

(c) *What requirements apply to 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 PSP must identify all safety hazards to be mitigated by the locomotive engineer.

(2) The PSP must 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 § 236.923(a)(2), develop failure scenarios which incorporate the safety hazards identified in the PSP, including the return of train operations to a fully manual mode;

(ii) Provide training, consistent with § 236.923(a), for safe train operations under all failure scenarios and identified safety hazards that affect train operations;

(iii) Provide training, consistent with § 236.923(a), for safe train operations under manual control; and

(iv) Consistent with § 236.923(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 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.

■ 12. Amend Appendix A to part 236 by adding an entry for § 236.18 and adding entries for subpart H as follows:

APPENDIX A TO PART 236.—CIVIL PENALTIES [1]

Section	Violation	Willful violation
Subpart A—Rules and Instructions, All Systems		
* * * * * * *		
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
* * * * * * *		
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:		

APPENDIX A TO PART 236.—CIVIL PENALTIES [1]—Continued

Section	Violation	Willful violation
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

[1] The Administrator reserves the right to assess a civil penalty of up to $27,000 per day for any violation where circumstances warrant. See 49 CFR part 209, appendix A.

■ 12a. Add 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 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 system that operates over a life-cycle of 25 years or greater. 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 safety-critical assessment of each product must include all of its interconnected subsystems and components and, where applicable, the interaction between such subsystems.

(c) *How is the previous condition computed?* Each subsystem or component of the previous condition must be analyzed with a Mean Time To Hazardous Event (MTTHE) as specified subject to a high degree of confidence.

(d) *What major risk characteristics must be included when relevant to 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;

(2) Total number of trains and movement density;

(3) Train movement operational rules, as enforced by the dispatcher and train crew behaviors;

(4) Wayside subsystems and components; and

(5) Onboard subsystems and components.

(e) *What other relevant parameters must be determined for the subsystems and components?* The failure modes of each subsystem or component, or both, must be determined for the integrated hardware/software (where applicable) as a function of the Mean Time To Failure (MTTF) failure restoration rates, and the integrated hardware/software coverage of all processor-based subsystems or components, or both. Train operating and movement rules, along with components that are layered in order to enhance safety-critical behavior, must also be considered.

(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 an 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) MTTHE compliance verification and validation must be based on the assessment of the design for verification and validation process, historical performance data, analytical methods and experimental safety-critical performance testing performed on the subsystem or component. The compliance process must be demonstrated to be compliant and consistent with the MTTHE metric and demonstrated to have 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 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 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?* (1) The railroad shall document any assumptions regarding the reliability or availability of mechanical, electric, or electronic components. Such assumptions must include MTTF projections, as well as Mean Time To Repair (MTTR) projections, unless the risk assessment specifically explains why these assumptions are not relevant to the risk assessment. The railroad shall document these assumptions in such a form as to permit later automated comparisons with in-service experience (*e.g.*, a spreadsheet).

(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. The documentation shall be in such a form as to facilitate later comparisons with in-service faults.

■ 13. Add Appendix C to part 236 to read as follows:

Appendix C to Part 236—Safety Assurance Criteria and Processes

(a) *What is the purpose of this appendix?* This appendix seeks to promote full disclosure of safety risk to facilitate minimizing or eliminating elements of risk where practicable by providing minimum criteria and processes for safety analyses conducted in support of PSPs. The analysis required by this appendix is intended to minimize the probability of failure to an acceptable level, helping to optimize the safety of the product within the limitations of the available engineering science, cost, and other constraints. FRA uses the criteria and processes set forth in this appendix to evaluate analyses, assumptions, and conclusions provided in RSPP and PSP documents. An analysis performed under this appendix must:

(1) Address each area of paragraph (b) of this appendix, explaining how such objectives are addressed or why they are not relevant, and

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

(b) *What categories of safety elements must be addressed?* The designer shall address each of the following safety considerations when designing and demonstrating the safety of products covered by subpart H of this part. In the event that any of these principles are not followed, the PSP 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) *Normal operation.* The system (including all hardware and software) must demonstrate safe operation with no hardware failures 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. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

(2) *Systematic failure.* It must be shown how the product is designed to 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.

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

(ii) 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 any physical appliance.

(iii) 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 any physical appliance.

(4) *Common Mode failure.* Another concern of multiple failure 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.

(5) *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.

(6) *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.

(7) *Software.* Software faults must not cause hazards categorized as unacceptable or undesirable.

(8) *Closed Loop Principle.* The product design must require positive action to be taken in a prescribed manner to either begin product operation or continue product operation.

(9) *Human Factors Engineering:* 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.

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

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

(ii) CENELEC Standards as follows:

(A) EN50126: 1999, Railway Applications: Specification and Demonstration of

Reliability, Availability, Maintainability and Safety (RAMS);

(B) EN50128 (May 2001), Railway Applications: Software for Railway Control and Protection Systems;

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

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

(iii) ATCS Specification 140, Recommended Practices for Safety and Systems Assurance.

(iv) ATCS Specification 130, Software Quality Assurance.

(v) AAR-AREMA 2005 Communications and Signal Manual of Recommended Practices, Part 17.

(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.

(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.

■ 14. Add Appendix D to part 236 to read as follows:

Appendix D to Part 236—Independent Review of Verification and Validation

(a) *What is the purpose of this appendix?* This appendix provides minimum requirements for independent third-party assessment of product safety verification and validation pursuant to subpart H 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 the applicable railroad's RSPP, the product PSP, the requirements of subpart H of this part, and any other previously agreed-upon controlling documents or standards.

(b) *What general requirements apply to the conduct of third party assessments?* (1) 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 should not engage in design efforts, in order to preserve the reviewer's independence and maintain the supplier's proprietary right to the product.

(2) 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.

(c) *What must be done at the preliminary level?* 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 product. At a minimum, the reviewer shall compare the supplier processes with acceptable 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 the adequacy of the railroad's RSPP, the PSP, and any other documents pertinent to the product being assessed.

(d) *What must be done at the functional level?* (1) The reviewer shall analyze the Preliminary Hazard Analysis (PHA) for comprehensiveness and compliance with the railroad's RSPP.

(2) 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 the railroad's RSPP.

(e) *What must be done at the implementation level?* The reviewer shall randomly select various safety-critical software modules for audit to verify whether the requirements of the RSPP 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 RSPP.

(f) *What must be done at closure?* (1) The reviewer shall evaluate and comment on the plan for installation and test procedures of the product for revenue service.

(2) 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:

(i) Reviewer's evaluation of the adequacy of the PSP, including the supplier's MTTHE and risk estimates for the product, and the supplier's confidence interval in these estimates;

(ii) Product vulnerabilities which the reviewer felt were not adequately mitigated, including the method by which the railroad would assure product safety in the event of a hardware or software failure (*i.e.*, how does the railroad assure that all potentially hazardous failure modes are identified?) and the method by which the railroad addresses comprehensiveness of the product design for the requirements of the operations it will govern (*i.e.*, how does the railroad assure that all potentially hazardous operating circumstances are identified? Who records any deficiencies identified in the design process? Who tracks the correction of these deficiencies and confirms that they are corrected?);

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

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

(v) A listing of each RSPP procedure or process which was not properly followed;

(vi) Identification of the software verification and validation procedures for the product's safety-critical applications, and the reviewer's evaluation of the adequacy of these procedures;

(vii) Methods employed by the product manufacturer to develop safety-critical software, such as use of structured language, code checks, modularity, or other similar generally acceptable techniques; and

(viii) 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.

■ 15. Add Appendix E to part 236 to read as follows:

Appendix E to Part 236—Human-Machine Interface (HMI) Design

(a) *What is the purpose of this appendix?* The purpose of this appendix is to provide HMI design criteria which will minimize negative safety effects by causing designers to consider human factors in the development of HMIs.

(b) *What is meant by ''designer'' and ''operator''?* 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 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 signal or train control product subject to subpart H of this part.

(c) *What kinds of human factors issues must designers consider with regard to the general function of a system?*

(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 shall consider at 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 they require an operator to take action; and

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

(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) *Limited memory and ability to process information.*

(i) HMI design must minimize an operator's information processing load. To minimize information processing load, the designer shall:

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

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

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

(ii) HMI design must minimize the load on an operator's memory.

(A) 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.

(B) 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.

(4) *Miscellaneous Human Factors Concerns.* System designers shall:

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

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

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

(d) *What kinds of HMI design elements must a designer incorporate in the development of on-board train displays and controls?*

(1) *Location of displays and controls.* Designers shall:

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

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

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

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

(v) Group similar controls together;

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

(vii) 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); and

(viii) Design controls to allow easy recovery from error.

(2) *Information management.* HMI design must:

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

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

(iii) Design for display luminance of the foreground or background of at least 35 cd/m^2 (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);

(iv) Design the interface to display only the information necessary to the user;

(v) Where text is needed, using short, simple sentences or phrases with wording that an operator will understand;

(vi) 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;

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

(viii) 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;

(ix) Group items that belong together;

(x) 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;

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

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

(xiii) With respect to information entry, avoid full QWERTY keyboards for data entry; and

(xiv) Use digital communications for safety-critical messages between the locomotive engineer and the dispatcher.

(e) *What kinds of HMI design elements must a designer consider with respect to problem management?* (1) HMI design must enhance an operator's situation awareness. An operator must have access to:

(i) Knowledge of the operator's train location relative to relevant entities;

(ii) Knowledge of the type and importance of relevant entities;

(iii) Understanding of the evolution of the situation over time;

(iv) Knowledge of the roles and responsibilities of relevant entities; and

(v) Knowledge of expected actions of relevant entities.

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

(3) HMI design must support contingency planning.

Issued in Washington, DC on February 24, 2005.

Robert D. Jamison,

Acting Administrator, Federal Railroad Administration.

[FR Doc. 05–3955 Filed 3–2–05; 8:45 am]

BILLING CODE 4910–06–P