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: Notice of proposed rulemaking.

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

DATES: *Written Comments.* Comments must be received by October 9, 2001. Comments received after that date will be considered to the extent possible without incurring additional expense or delay.

Public Hearings: Upon specific request, FRA will hold public hearings as appropriate to receive oral comments from any interested party.

ADDRESSES: Comments should be sent to the Docket Clerk, Docket Management System, U.S. Department of Transportation Room PL 401, 400 Seventh Street, SW., Washington, DC 20590–0001. If you wish to receive confirmation of receipt of your written comments, please include a self-addressed, stamped postcard.

The docket management system is located on the Plaza level of the Nassif Building at the Department of Transportation at the above address. You can review public dockets there between the hours of 9 a.m. and 5 p.m., Monday through Friday, except federal holidays. You can also review comments on-line at the DOT Docket Management System web site at *http://dms.dot.gov.*

You may submit comments electronically by accessing the Docket Management System web site at *http://dms.dot.gov* and following the instructions for submitting a document electronically.

FOR FURTHER INFORMATION CONTACT: William H. Goodman, Staff Director, Railroad Signal Program, Office of Safety, FRA, 1120 Vermont Avenue, NW, Washington, DC 20590 (telephone: 202–493–6325); Grady C. Cothen, Jr., Deputy Associate Administrator for Safety Standards, FRA, 1120 Vermont Avenue, NW, Mail Stop 25, Washington, D.C. 20590 (telephone: 202–493–6302); Cynthia B. Walters, Office of Chief Counsel, FRA 1120 Vermont Avenue, NW, Mail Stop 10, Washington, DC 20590 (telephone: 202–493–6064); or David T. Matsuda, Office of Chief Counsel, FRA, 1120 Vermont Avenue, NW, Mail Stop 10, Washington, DC 20590 (telephone: 202–493–6046).

SUPPLEMENTARY INFORMATION:

I. Statutory Background

The Federal Railroad Administration (FRA) has broad statutory authority to regulate all areas of railroad safety. 49 U.S.C. 20103(a); 49 CFR 1.49. 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. 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 in large part governed the installation and removal of signal equipment for most of the previous century.

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. For example, in the area of railroad signal and train control systems, FRA has issued regulations, found at 49 CFR part 236 (''Part 236''), addressing the security of signal apparatus housings (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 shall be parts located in Title 49 of the Code of Federal Regulations.

II. 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 positive train control (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 needed to facilitate realization of the potential of electronic control systems and for safety and efficiency.

FRA has already used its 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 (UP)/Burlington Northern Santa Fe (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. (CSX) Communication-Based Train Management (CBTM) project in Georgia, and the Alaska Railroad PTC project. FRA recently 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 responsible tests, demonstrations, and implementations, the need for controlling principles in this area is becoming increasingly obvious. This rulemaking provides the forum for identifying and codifying those principles.

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.'' The RSERA mandated that the Secretary conduct a safety inquiry to assess, among other areas, the status of advanced train control systems and the need for federal standards to ensure that such systems provide for positive train separation and are compatible nationwide. FRA conducted such an inquiry and submitted a comprehensive Report to Congress on July 8, 1994.

As part of this Report, FRA called for implementation of an action plan to deploy PTC systems (''Railroad communications and Train Control,'' FRA, July 1994). 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.

Following through on the Report, the FRA 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 the Pacific Northwest, Michigan, 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 (''Administrator'') asked the Railroad Safety Advisory Committee to address several issues involving PTC.

III. Railroad Safety Advisory Committee (RSAC)

A. RSAC

Since 1993, FRA has been taking action to promote earlier and more extensive participation by all interested parties in the agency's regulatory processes. That year, the Administrator conducted a series of roundtables on all aspects of FRA's safety program. FRA initiated its first formal negotiated rulemaking in 1994 on the topic of roadway worker safety.

FRA also conducted outreach and a review of its regulatory program under the President's Regulatory Reinvention Initiative and the National Performance Review. FRA concluded that railroad safety would be best served if the agency varied its traditional ''hear and decide'' regulatory style to a new one founded on consensus among those who are benefitted and burdened by the agency's regulations. Implicit in this change is the concept that decisions regarding the best approach to resolution of safety issues should be made with the full participation of all affected parties.

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 Transit Association (APTA)
American Short Line and Regional Railroad Association (ASLRRA)
American Train Dispatchers Department/BLE (ATDD/BLE)
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 Employes (BMWE)
Brotherhood of Railroad Signalmen (BRS)
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) (non-voting)
League of Railway Industry Women (non-voting)
National Association of Railroad Passengers (NARP)
National Association of Railway Business Women (non-voting)
National Conference of Firemen & Oilers
National Railroad Construction and Maintenance Association
Amtrak
Railway Progress Institute (RPI)
Safe Travel America
Secretaria de Communicaciones y Transporte (non-voting)
Sheet Metal Workers International Association
Tourist Railway Association Inc.
Transport Canada (non-voting)
Transport Workers Union of America (TWUA)
Transportation Communications International Union/BRC (TCIU/BRC)
United Transportation Union (UTU)
National Transportation Safety Board (NTSB) (non-voting)
Federal Transit Administration (FTA) (non-voting)

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 recommendations to FRA for action on the task. These recommendations are developed by consensus. 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. If the working group is unable to reach consensus on recommendations for action, FRA moves ahead to resolve the issue through traditional rulemaking proceedings.

Recommendations from RSAC come in all varieties. RSAC may recommend continued implementation of existing measures, voluntary initiatives by individual parties, concerted voluntary initiatives by several parties, amendment of existing regulations, new regulatory requirements, or enactment

of legislation, as appropriate. The advice and recommendations of RSAC form the basis for this proposed rule.

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.

B. The PTC Working Group

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

AAR, including members from
BNSF
Canadian National
Conrail
CSX
Metra
Norfolk Southern Railway Company
UP
Amtrak
AASHTO
APTA
ASLRRA
ATDD/BLE
BLE
BMWE
BRS
FRA
FTA (non-voting)
HSR/MAG LEV
IBEW
NTSB (non-voting)
RPI
UTU

In order to efficiently accomplish the three tasks assigned to it involving PTC issues, the PTC 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 on September 8, 1999. Report of the Railroad Safety Advisory Committee to the Federal Railroad Administrator, ''Implementation of Positive Train Control Systems,'' (September 8, 1999). The Data and Implementation Task Force will be involved in monitoring implementation of PTC technology on the joint Illinois/AAR/UP/FRA project.

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.

In addition to providing assistance from FRA staff and staff from the Volpe National Transportation Safety Center, 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.

C. The Standards Task Force

The Working Group, consisting of both the Data and Implementation Task Force and the Standards Task Force, held a meeting at Ponte Vedra Beach, Florida in November 1997 to set the direction of the Standards Task Force. An informal first meeting of the Standards Task Force was held in Washington DC on December 18, 1997, followed by the first formal meeting on February 25, 1998, in Fort Worth, Texas. The Standards Task Force is primarily responsible, with the FRA Office of Chief Counsel and Office of Safety, for drafting this proposed rule.

After the initial informal meeting, the Standards Task Force met almost every month until the last meeting in New Orleans, LA on June 28–29 of 2000. Much documentation was produced at these meetings, due to extensive discussions, presentations and tutorials. This documentation has been placed in the docket for this rulemaking.

The primary mission of the Standards Task Force was to develop regulations that would address the new PTC systems, as well as subsystems and components thereof. PTC systems were described as achieving three core functions: (1) Preventing train-to-train collisions (positive train separation); (2) enforcing speed restrictions, including civil engineering restrictions and temporary slow orders; and (3) providing protection for roadway workers and their equipment operating under specific authorities.

At each meeting, proposed standards were continually developed and modified. The text of the proposed regulation became known as the ''Master Draft.'' Four primary stakeholder groups worked on the Master Draft and presented their own views and opinions as to what should be included in the regulations. As such, consensus was very difficult to obtain. The four stakeholder groups involved were: (1) The federal government, (2) railroad management, (3) railroad labor, and (4) railroad signal and train control system suppliers. The first three groups had voting powers. The supplier group did not have voting powers, but their input was essential and valuable to the other interest groups, especially railroad management, their primary customers. All Standards Task Force meetings were open to all interested parties, and on the average, 30 to 35 people attended. The final two meetings recorded over 50 attendees each. Any attendee was considered a member of the Standards Task Force and had the right to express an opinion at the meeting. However, when consensus was called for, only actual voting members from the PTC Working Group were counted.

In December 1999, the Standards Task Force reached consensus on most outstanding issues. Chiefly, these included the adoption of risk assessment criteria, requirements for independent third party review of validation and verification, applicability of the proposed rule to existing systems, life cycle recordkeeping and reporting, and related matters.

On June 29, 2000, the Standards Task Force presented its consensus recommendation to the entire working group. The PTC Working Group accepted the recommendation with minor changes and forwarded its consensus recommendation to RSAC, which approved it on September 14, 2000.

IV. Major Issues

A. Why a Performance-Based Approach?

What is a Performance Standard?

During the Standards Task Force discussion, 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 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 that the group pursue higher-level performance standards. Supplier and labor representatives agreed to this approach, and FRA has endeavored to support the Standards Task Force in pursuing it.

Early in the deliberations of the Standards Task Force, carrier representatives requested that FRA arrange presentations on the use of performance standards in lieu of prescriptive regulations. The group heard from representatives of the Research and Special Programs Administration (RSPA), Federal Highway Administration's Office of Motor Carrier Safety (now Federal Motor Carrier Safety Administration (FMCSA)), 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. The Working Group 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., 49 CFR 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-related 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 (though just how specific the requirements should remain is one of the subjects of this proceeding).

Criteria for Evaluation of Performance-Related Approach

The discussion that follows identifies some of the general considerations that apply to use of performance standards and some of the practical factors that come into play with respect to the safety of processor-based signal and train control technologies.

In response to the report of the Vice President's Commission on Aviation Safety and Security, the Federal Aviation Administration (FAA) published a brief ''Performance-Based Regulations Guide'' (October 31, 1997). That guide notes four ''substantive criteria'' that can be used to determine whether regulations can be written in a performance-based manner:

1. Can the regulatory requirement be stated in terms of a practical goal that can be understood by an individual or company (e.g., meeting a prescribed climb gradient with one engine inoperative)?
2. Will a regulation stated in performance terms be enforceable?
3. Will a performance-based regulation discriminate against smaller companies?
4. Is it possible to establish an equivalency rule that will itself be considered a performance-based regulation? (In FAA terminology, ''an equivalency rule'' is one that is based upon a command-and-control requirement but allows the regulated party to demonstrate that an alternative approach provides an equivalent level of safety.)

The FAA guide noted performance-based regulations should not be used if:

1. Congress has mandated a specific outcome (e.g., ''no smoking'' on domestic flights).
2. The standard would be so vague as to be unenforceable (e.g., ''fly safely'').
3. The FAA cannot agree on an acceptable alternative to a command-and-control standard (e.g., the age 60 rule [for air transport pilots] could be eliminated only if the FAA could prescribe medical and flight testing standards that would provide an equivalent level of safety).

These criteria are generally applicable to the issue presented by this proposal, and other possible concerns can be added. For instance, what if administration of a performance standard would involve too much cost to all regulated entities, small entities only, or the government? What if the performance standard is clear, but verifiable only after the fact and thus enforceable only in a reactive sense? What if the standard is very clear, but the analytical techniques needed to

verify compliance are poorly developed or are not validated?

FRA has identified several criteria of its own with respect to promulgating a performance standard for this area of regulation: simplicity, relevancy, reliability, cost, and objectivity.

First, FRA feels the standard should be simple, because it will apply to many regulated entities. If the standard requires complex mathematics, there may be no way for many of the entities to comply, and if complicated enough, the standard may be beyond FRA's capacity to enforce. For instance, the Standards Task Force has been exposed to many briefings on mathematical techniques used to measure product safety. Often, the mathematics were extremely complicated, the issues surrounding selection of a model so esoteric that only a small fraction of the expert population present fully understood the issues, and at no point was there a consensus that any particular technique was technically superior.

Second, FRA feels the standard should be relevant with respect to safety. There may be many convenient measurable qualities of processor-based systems which are not relevant to safety. For example, the mean time to repair a product subsystem may or may not necessarily be relevant to safety, depending upon the backup method of operation in place.

Third, FRA believes the standard should be reliable in that the test applied should yield similar results each time it is applied.

Fourth, FRA believes demonstrating compliance with the standard should not be unduly expensive. Train control systems have a very good safety record. The cost of proving compliance with the standard should not cost more than the benefits it will bring. Furthermore, a standard could be so exacting that it would prevent the deployment of systems which would very likely improve safety, but which do not meet some extremely difficult or expensive test. Thus a purported safety standard might actually impose safety costs.

Fifth, FRA feels the standard should be objective. A completely objective standard would allow for compliance to be determined through scientific study or investigation. This is critical from a regulatory perspective, because FRA feels it would not be fulfilling its safety mission if it could not verify compliance with the performance standard. Also, an objective standard would allow for sound business planning with respect to budgeting for and development of processor-based systems. Thus, FRA can realize additional safety benefits from this standpoint.

Development of the Proposed Standard

The Standards Task Force considered only two different performance standards, yet determining an adequate method for demonstrating compliance was the key factor in the Standards Task Force's final decision.

The first standard proposed for discussion by the Standards Task Force was a standard which would have required that the implementation of proposed systems lead to safety improvements of 33% to 50%. This standard was proposed in order to address the uncertainties involved in the safety determinations. The theory behind the proposal was that an actual increase in safety by a discrete relative amount would overcome any uncertainties involved in the safety assessment process. In addition to the objectivity problems involved in not necessarily requiring a certain level of confidence in the safety measurements, the most disconcerting issue to the group was the cost of such a standard. It would impose burdensome safety and operational costs. The safety costs would result primarily from railroads not being able to replace products with those which would improve safety by less than the desired margin. The operational costs would result from not being able to replace a product with one that was equally as safe, but less costly. These shortcomings were too severe for the Standards Task Force to warrant further consideration of this option.

The only other performance standard considered by the Standards Task Force was the one which led to the proposed rule: that new products must not degrade safety. This standard was not formally agreed to by the Standards Task Force until a means for demonstrating compliance could be agreed upon. The remainder of the discussions focused on the various ways in which compliance with this standard could be determined, and which of them is the most appropriate.

The first proposal under this standard would have required a comparison of the sample means of the distributions of risk for the proposed product and the current system. This proposal would require demonstration with a minimum ninety-five percent confidence level that the likelihood that the distribution of risk for the proposed system is not less than the sample mean for the current system. The Standards Task Force found cost to be the most serious concern with this proposal. For relatively simple products this approach may be cost-effective. It would be moderately expensive, as it requires some modeling of the risk, but the cost of modeling might still be less than the costs of complying with a specification standard. The most significant costs would be incurred when a proposed system takes advantage of current-generation, high-capability processors. The expense of computing time required to generate statistically significant modeling results would be prohibitive.

A slightly different approach would be to test the standard deviations of the differences in sample means. This approach is not much more complicated than simply testing against the standard deviations. The cost would be roughly the same, however, this approach would pose reliability problems. If the number of simulation cycles were held to a fixed ratio between cycles for the current system and cycles for the proposed product, the standard deviation of the sample mean would decrease in proportion to the square root of the number of simulation cycles. Furthermore, the looseness of the assumptions would affect reliability of this approach as a measurement tool. There could also be significant problems with non-random re-selection of paths in simulations.

The next approach proposed was to weight each risk calculation by a factor of uncertainty, and then run the simulation to see what the relationship is between current risk levels and levels of risk associated with use of the proposed product. This approach would require a higher level of confidence for a lower subjective confidence in the underlying assumptions. This option is more complex than any yet discussed by the Standards Task Force, and does not appear to be either reliable or objective. The Standards Task Force ultimately concluded that this test is too subjective for their purpose.

Also suggested was an approach utilizing statistics of extremes, or extreme value theory. This objective technique is favored for risk analysis in civil engineering and environmental science applications and is designed to overcome the problems which arise when using traditional distribution models to analyze low probability, high consequence events. It is sufficiently complex that there was no consensus in the group as to its effectiveness for train control applications, although the University of Virginia continues to provide the group with more information on this technique. An informal survey of group members revealed that fewer than one tenth of an expert group claimed to be familiar with extreme value analysis. Thus, the Standards Task Force concluded

unfamiliarity with this approach within the industry would probably make it expensive to require.

The final mathematical approach suggested was described as a Bayesian belief network. This is also a complicated test, which appears not totally objective. This approach would require the railroad to show by some high evidentiary standard, such as ''demonstrating to a high degree of confidence,'' that the proposed product would result in no loss of safety. It is this final test which FRA proposes. The Standards Task Force has developed more specific criteria for satisfying the performance standard under this approach using current safety engineering practices and principles within the industry.

Although advantages of and concerns with the proposed standard are addressed in the sections which follow, FRA seeks comments addressing the decisions reached by the Standards Task Force concerning the various standards and compliance methodologies considered and rejected.

Advantages of a Performance-Based Standard

This NPRM presents the highest level performance requirements ever attempted by FRA. To informed advocates of performance-based regulations, the reasons for taking this course are obvious. The emerging technologies documented in the RSAC's Report to the Administrator (''Implementation of Positive Train Control Systems,'' September 8, 1999), reflect an extensive array of electronic applications, including short-range radio frequency (RF) data links (transponders), medium-range RF data links, train location systems employing GPS/DGPS positioning supported by inertial guidance and track database analysis, and logic controllers placed at central office locations, on the wayside and onboard trains. Inputs may be derived from a variety of on-board systems, automatic equipment identification systems, two-way end-of-train telemetry, existing signal and train control systems, and other sources. Additional technologies are on the horizon, and others will no doubt emerge between the date of publication of a final rule in this proceeding and the next revision of the regulations by FRA.

While some new train control systems may not yield all of the same safety benefits that are supported by traditional track circuits (e.g., detection of some broken rails), they may be capable of very nearly eliminating train-to-train collisions and addressing the other PTC core functions. Data derived from train control applications may be used for improved train management, crew management, and other business purposes. Ultimately, PTC technology may permit the transfer of train movement information for use in providing warning at highway-rail grade crossings under conditions that are, today, prohibitively expensive.

In short, the future benefits of emerging railway electronic systems will be substantial, and suppliers and carriers will need a great deal of flexibility to avoid inadvertent limitations on the growth of important safety systems. This rulemaking was commenced to facilitate introduction of these new technologies. A performance-based approach should be the most powerful means of accomplishing that objective because it would:

- Provide the maximum flexibility to design capable systems, increasing the likelihood that all possibilities will be carefully explored;
- Permit designers to optimize systems to address safety and other needs, making systems more attractive to those making capital allocation decisions; and
- Avoid inappropriate requirements that could drive up costs and put the technology out of reach for years to come.

Concerns With a Performance-Based Standard

This notice embodies a very high-level approach to performance standards that would offer unprecedented flexibility for carriers to design and deploy new signal and train control technologies. At the same time, it would require extensive documentation of the safety of the system prior to its introduction in revenue service. This approach has many profound advantages, and notable disadvantages, that deserve scrutiny in this rulemaking.

FRA has also noted significant obstacles to successful implementation of performance standards in this context, as well as reservations with respect to the utility of such standards. These concerns are sufficient to warrant caution and a vigorous public debate.

The first concern that has arisen is the static nature of a fixed performance standard grounded in current safety performance levels. As noted above, this proceeding is intended to facilitate safety improvement through accelerated introduction of new technology. The proposed performance standard described below, which basically provides that the safety of a new system may not fall below the base condition (existing technology, with certain adjustments), sets a modest objective for suppliers and railroads. However, progress is not the inevitable result of technological innovation. It is at least theoretically possible for a railroad to claim greater efficiencies associated with new technology, add modest safety enhancements that go beyond the capabilities of existing signal technology, but delete certain functionalities associated with the existing system or implement the system in a manner that includes significant safety vulnerabilities. The net result could be cost savings with no advance in safety. Yet, unlike today, FRA would lack leverage under the regulations to insist that known vulnerabilities in the system be corrected, even if that could be done on a highly cost effective basis. (FRA would retain its general authority under the Signal Inspection Act, but the extent to which that authority might be impaired could only be determined after extensive litigation, should its exercise be challenged.)

The thought that a performance standard might stagnate safety improvements is not a fanciful concern. Since economic deregulation of the railroad industry (signified most notably by enactment of the Staggers Rail Act of 1980), railroads have progressed toward profitability principally by cutting costs. Strong intermodal competition has caused the railroads to turn much of the resulting savings back to shippers in the form of reduced contract rates. Particularly in the wake of major mergers and consolidations (a condition applicable to each of the four largest railroads today), the pressure from the financial community for cost reduction is particularly strong. This has sometimes led to management decisions based on short-term considerations. FRA regularly deals with the effects of this phenomenon in the context of Safety Assurance and Compliance Programs on the various properties.

Clearly, the railroads have managed to improve their overall safety performance during the past 20 years while also cutting costs, in part by using technology to good advantage. However, the low-hanging fruit is largely gone. Managers and employees are increasingly asked to do more with less, which is a confining business practice. Properly implemented, new signal and train control technology can help reduce workload requirements while also improving asset utilization. Improperly implemented, the technology could stagnate safety improvements.

Second, doubt remains whether the relevant technical, scientific, and railroad signaling communities are fully

prepared to support implementation of this rule. FRA has funded significant research into the safety of processor-based systems. *See, e.g.,* ''Analytical Methodology for Safety Validation of Computer Controlled Subsystems,'' (Luedeke, John, (Battelle) for Volpe National Transportation Systems Center; DOT–VNTSC–FRA–95–8 (April 1994)). Administration of existing regulations, including consideration of waivers associated with novel train control proposals, has provided FRA with the opportunity to become familiar with strengths and limitations of the safety programs of major signal suppliers. Field compliance efforts have provided a reasonably good view of railroads' efforts to implement processor-based technologies. FRA's observations from this experience follow.

The field of system safety for safety-critical control systems is relatively young and remains in flux. Military Standard 882C, ''System Safety Program Requirements'' (U.S. Department of Defense; January 18, 1993), provides an overall framework for safety planning and analysis. A growing body of literature documents good practice in the field. *See, e.g.,* Leveson, Nancy G., ''Safeware: System Safety and Computers,'' Addison Wesley Publishing Company, Inc., 1995. FRA purchased and distributed to Standards Task Force members copies of ''Safety-Critical Computer Systems'' (Storey, Neil; Addison-Wesley Longman (Harlow, England 1996)), a text addressing the subject matter in a way characterized as suitable for a final-year undergraduate or masters-level program in engineering. The FAA, the Nuclear Regulatory Commission, and other Federal agencies have addressed this issue in various ways and continue to conduct relevant research. Parallel efforts internationally include the European Committee for Electrical Standardization (CENELEC) standard prEN50129 ''Railway Applications—Safety-Related Electronic Systems for Signaling,'' (May 18, 1998).

Railroad signal suppliers maintain a strong emphasis on the safety of their systems. However, formal processes to conduct and document safety analyses for new products are not uniform in their content; and FRA is aware of departures from what might be deemed acceptable within the framework of a rule implementing the proposals set forth below. In general, suppliers employ varying safety assurance concepts for their products and are not currently able to provide quantitative information concerning the projected life-cycle safety performance of new products. The vigorous emphasis on more formal methods of safety assurance in the supply community is exemplified by the recent adoption by the Institute of Electrical and Electronic Engineers, Inc. (IEEE), of the new ''Standard for the Verification of Safety for Processor-based Systems Used in Rail Transit Control'' (No. 1483). The lack of complete consensus on the issue of proofs of safety is perhaps best exemplified by the fact that the IEEE standard just referenced does not address validation of these systems.

Recognizing that any performance standard must provide a level playing field for the supply community and clear decisional criteria for FRA's review of safety documentation, FRA asked the Standards Task Force to focus specifically on the requirements for verification and validation and the associated quantization of safety (further discussed below). Although the supply community representatives were able to agree with other Standards Task Force members on general principles that should apply to these safety processes and the metric of Mean Time to Hazardous Event (MTTHE), suppliers were not able to agree to provide estimates of MTTHE based on fully quantitative inputs derived from uniform analytical methods. The possibility remains, therefore, that estimates of residual risk from different suppliers might have different meanings and be based on differing levels of confidence. As public comment is received and considered, FRA will continue to work with the parties to ensure that information provided in support of various products is reasonably comparable.

FRA has also funded research into the application of risk assessment techniques to railroad operations and has made use of risk studies in the development of its own rules and in the evaluation of system safety estimates presented by various parties. Although FRA decision-making with respect to safety has always been founded on a keen appreciation for the elements of risk (event likelihood, severity, and an appropriate means for normalizing exposure), FRA recognizes that future advances in safety and transportation efficiency will necessitate a heavier reliance on often complex risk assessment techniques, as well as system safety principles. Quantitative risk assessments can enlighten decision making by taking into consideration a variety of relevant factors, providing a means of testing the sensitivity of key assumptions, and projecting the risk environment into the future. In an ideal circumstance, risk assessment may help identify critical system safety decisions and shed light on their mitigation well before the potential for hazardous events is realized in the field.

However, at the outset it must be said that use of risk assessment to determine compliance with performance criteria embodied in a regulation presents an awkward problem. Practitioners of risk assessment are the first to point out that they do not purport to provide information that will predict actual levels of performance. Rather, they provide analysis that suggests the ''relative safety'' of the projected system in relation to a base case construct against which it is evaluated. This is a particularly powerful technique to improve the safety of a system, if properly executed. But the results do not constitute direct proof that a particular level of safety will be achieved.

Obviously, this problem could be ''solved'' by simply requiring that an analysis meeting certain criteria show an improvement in safety. However, FRA believes that this approach would ask the wrong question and result in an increasingly parochial focus on the techniques of risk assessment and their proper execution, to the exclusion of the concrete safety issues presented by particular systems. FRA was not established to regulate risk assessment techniques, and attempting to do so would only inhibit the growth of the discipline. Accordingly, FRA has insisted that the proposed performance criterion be stated in absolute terms, with latitude afforded to scale the analytical effort to the problem at hand. Obviously, in the end FRA would have to be convinced that the particular showing was persuasive with respect to the likelihood that the new system would meet or exceed the safety performance of the existing system.

Further, quantitative risk assessment as applied to the safety of railroad operations is best viewed as an art, rather than a science. A proper analysis must correctly describe salient elements of the operating system, correctly assess the contribution of the risk dimension under review to key scenarios, accurately estimate the frequency with which the risk will arise, accurately describe the severity of hazardous events that may occur, and fairly evaluate the impact of mitigating measures on the prevention, or reduction in severity, of the hazardous event. This requires that the analyst(s) be fully conversant with the railroad operating system, that input data be available (and be properly selected if various data are available), that the analysis be structured to produce a credible result, and that the result be

appropriately characterized. There are challenges associated with each of these steps.

FRA is also concerned that a requirement for a risk assessment based on probability or likelihood will refocus safety efforts during development from optimization to post-design justification. That is, FRA fears that the focus will shift to proving that the product is safe enough after it has been designed. This concern is fueled by such facts as: (1) Subsystems and components involving software and/or human factors do not readily lend themselves to risk quantization as electro-mechanical ones do, (2) risk calculations for current operations will most likely be limited in precision, and (3) early FRA involvement in the product development process is not mandated. As William D. Ruckelshaus, former two-time Director of the U.S. Environmental Protection Agency (EPA), has pointed out, ''risk assessment data can be like the captured spy; if you torture it long enough, it will tell you anything you want to know.'' Leveson at 60.

In practice, FRA has had occasion to substantially discount the value of risk assessments in some cases, while relying heavily on the results (together with other information) in other cases. FRA expects that the quality of risk assessment practice will improve over time, as experience is gained and as peer review strengthens the quality of analysis.

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 an ''Axiomatic Safety-Critical Assessment Process'' (ASCAP). At the request of the Standards Task Force, FRA engaged the University of Virginia to develop the ASCAP model as a risk assessment ''toolkit'' for use in implementing this proposed rule. The initial challenge for the ASCAP team and contractor has been to describe the relative safety of 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 will be the safety of operations on the same line should a traffic control system be installed. The second comparison case will be implementation of the proposed CBTM system, an innovative technology that addresses the PTC core functions.

As this proposed rule was being finalized for review and publication, the ASCAP effort was progressing toward generation of the base case and an initial comparison case. The University of Virginia principal researcher continued to meet with the ASCAP team providing peer review and support for the project. Data was being assembled and reviewed for suitability. A Human Factors Team had been established to assist in formulating input assumptions with respect to the anticipated actions of employees under various conditions associated with the three methods of operations.

FRA believes that the ASCAP model (more fully described below) will represent a significant step forward in the quality of risk assessment methodologies related to train control. If successful, the technique may provide a level of analytical refinement significantly exceeding other known techniques. However, the success of this effort is not inevitable, given the degree of technical difficulty, the relative paucity of detailed data available for use within the model, and the uncertainties with respect to the role of human factors under the three cases. (For instance, CSXT and it employees who will be responsible for maintenance of various aspects of the system have not had experience with respect to maintenance of CBTM in the field. It may be difficult to project all failure modes that could be associated with routine maintenance and with modification of the system over its life cycle.) While it should be possible to benchmark the estimated risk for the base case and the traffic control system against experience on the CSXT line and for similar operations nationally, being certain of the validity for the CBTM case would require extensive, long-term experience in revenue service.

Indeed, for many risk assessment problems, the base case will not be ''known'' in a statistical sense before the work begins because there will not have been sufficient exposure in the specific territory affected, under current or projected conditions, to make collision and other data representative of actual long-term performance. This will require somewhat elaborate construction of a base case scenario (as in the current CSXT ''dark territory'' case mentioned immediately above) to permit consideration of the extent to which local conditions may affect national statistics that could otherwise be applied to the problem.

The Standards Task Force has discussed the fact that some margin of error will be associated with both base and comparison cases in any risk assessment. The group has discussed the need to employ sensitivity analysis to determine the effect of key assumptions and the desirability of putting a value on the extent to which the underlying analysis supports confidence in estimated risk, expressed as a point value or range. After examining several options, the group agreed to a standard fairly characterized as one of reasonableness, with respect to the current state of the art.

Whatever formal risk values emerge from an assessment conducted in conformity with the proposed rule, some statistical variability would apply to post-implementation review of systems. This is true both because risk assessments will provide an imperfect view of a very complex reality, but also because the wide dispersion of the pertinent risk and the seemingly random nature of potentiating events (e.g., a maintenance of way employee leaving a switch open on the main line) make precise predictions impossible. For instance, take the case of removal of an existing automatic block system (ABS) and its replacement by a non-vital communication-based train control system overlaid on track warrant control. The safety documentation for this ''product,'' as reviewed under this proposed rule (including part 235), might show an actual accident history of 2 severe events in the last 20 years, an estimated base risk level of 2.5 such events, and a predicted accident frequency for the new system of one severe event over 20 years into the future. Should the actual experience under the new system (with no change in traffic levels) be one severe event and one moderate event in the first five years, this could indicate the emergence of risk factors not foreseen when the analysis was conducted or simply the occurrence of events well within the range of expected outcomes.

FRA is particularly concerned that, under these circumstances, the dialogue between the FRA and the railroad not proceed based only upon the narrow technical details of risk assessment. Instead, the dialogue should center around the extent to which the events that occurred involved unnecessary harm to employees or the public and require remedial action that is practical and cost effective. If the public is to be served, FRA should not be shackled by its own performance criteria, and *pro forma* compliance with risk assessment should not bar inquiry into whether, as a practical matter, systems ''may be operated safely without unnecessary risk of personal injury.'' No amount of research is likely to make risk assessment a pure science, and no amount of litigation over it will protect employees and the public from patent hazards identified after the fact. FRA is not reassured by the discussion that led

to this proposal that this concern is frivolous, and FRA will not proceed with a final rule in this proceeding until a way has been found to resolve it.

FRA invites comments specifically addressing any of the agency's concerns detailed in this proposal.

Application to Part 235: Risk Assessments and Material Modification of Systems

This set of regulatory proposals includes performance-based rules for new signal and train control systems (including subsystems and components) but does not alter part 235, which governs applications for discontinuance or material modification of a signal system. FRA believes that risk assessment techniques can be helpful in evaluating applications for modification or discontinuance of existing signal systems. However, FRA is not prepared at this time to be bound by risk assessment outcomes in evaluating these applications.

In enacting the Signal Inspection Act, the Congress both authorized FRA to require installation of signal systems and required that FRA review their removal or any reduction in their effectiveness. FRA has been reluctant to order new signal system installations, because it appears that the market functions reasonably well due to the natural constraints associated with the growth of rail traffic. Railroads continue to install traffic control systems where capacity requires it, and those investments provide efficiencies that benefit the health of the railroads while also enhancing safety over the long term, both directly and indirectly.

FRA has also been reluctant, however, to allow removal of signal systems where current travel levels benefit from the safety that they provide, even if the agency would not order installation of a new system under the same circumstances. Tools such as the CRAM II model and the ASCAP model should assist FRA in determining the circumstances under which signalization is helpful. However, FRA is not convinced that the precision those tools can provide will always exceed in quality the judgment of railroad safety professionals who are intimately familiar with the territory and operations, particularly as applied to matters of limited scale.

FRA has also been reluctant to allow, and in recent years has been steadfastly opposed to allowing, elimination of automatic cab signal (ACS) and automatic train control (ATC) functions—functions that directly address, to a considerable degree, the issues of collision avoidance and protection of roadway workers. Certainly risk assessment techniques will be useful in the future to analyze proposals to replace ACS/ATC systems with communication-based PTC alternatives. However, FRA would not expect to seriously entertain arguments, based upon elaborate risk analysis, that less certain safety strategies or modest declines in traffic would support removal of ACS/ATC systems.

B. How Does This Proposal Affect Locomotive Electronics and Train Control?

This rule is prepared against a background of rapid and significant change in locomotive design. This change has direct implications for the future of train control systems onboard locomotives.

In the past, train control functions and systems for control of normal locomotive operating functions have been kept separate. Train control apparatus has applied independent of the normal throttle and braking functions, which were traditionally accomplished by mechanical and pneumatic controls used by the locomotive engineer. Cab signals and ATC/ATS appliances have included a separate antenna for interfacing with the track circuit or inductive devices on the wayside. The power supply and control logic for train control have been separate from other locomotive functions, and cab signals have been displayed from a special-purpose unit. Penalty brake applications have been accomplished by direct operation of a valve that accomplishes a service reduction of brake pipe pressure, and the train control system also functions to ''knock down'' the locomotive's tractive power. In keeping with this physical and functional separation, train control systems on board a locomotive have been considered exclusively within Part 236, rather than the locomotive inspection requirements of part 229.

Onboard locomotives, braking and throttle functions have traditionally worked independently, with discrete mechanical and pneumatic controls. As electronic systems were initially introduced, controls remained separate and distinct. Until recently, electronic controls have been packaged incrementally by various vendors (e.g., speed sensor vendor, brake system vendor, locomotive manufacturer). In locomotives that employ this arrangement, control functions may be distributed among several processors using proprietary software.

During the 1990's locomotive manufacturers (''original equipment manufacturers'' or ''OEMs'') began to integrate discrete functions, tapping certain inputs or outputs of the proprietary systems for informational or control purposes. Most new locomotives are controlled by microprocessors that respond to operator commands while making numerous automatic adjustments to locomotive systems to ensure efficient operation. In lieu of individual gages, operating parameters (such as speed, brake pipe pressure, and amperage) are displayed to the engineer on a single electronic display. The AAR has established Locomotive System Integration (LSI) criteria to promote compatibility among systems and uniformity in the information displayed to the locomotive engineer.

Currently, manufacturers are deploying central processors that may ''run'' a variety of systems simultaneously in a multi-tasking environment. While ''integration'' has been largely functional in the past, including the common display, the control systems themselves may be unified in the future.

Locomotive manufacturers are preparing more capable electronic platforms to support locomotive and train control functions, but to date FRA has taken the position that train control functions should remain separate. Historically, and within the context of existing ACS/ATC systems, train control functions have been required to be carried out in a failsafe manner by ''vital'' systems. Locomotive electronic controls, while designed with a high degree of attention to safety, have thus far not been demonstrated to fail safely with a high degree of reliability, and in individual cases unsafe failures have occurred. In effect, electronic control of locomotive functions has arisen in recent years without regulation, and in some cases products have been deployed prior to adequate analysis and testing. 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.

Very clearly, certain locomotive controls are highly safety-critical, and FRA is working with the OEMs to encourage adoption of formal safety methods in the design, verification and validation of locomotive systems. FRA is confident that, over the next few years, OEMs and their suppliers will succeed in improving the quality of safety-relevant locomotive electronic

systems. As that occurs, integration of train control functions with other on-board functions will be appropriate. Until that time, FRA believes that cab signal and train control functions, including innovative PTC technologies, should continue to operate independent of locomotive information and control systems. In the context of developing PTC projects, and with respect to application of required ACS/ATC systems on new locomotives, FRA will for the time being continue to insist upon separation of locomotive and train control functions (absent an affirmative showing by the OEM that essential functions are effectively isolated and implemented in a failsafe manner as required in part 236). However, both for today and the future, FRA sees value in use of the electronic display for cab signal and train control functions, if the generation of the relevant attributes of the display can be made failsafe (with the exception of the very low-probability possibility of a transient fault in the display itself).

FRA seeks comment on this issue and the circumstances under which the final rule should authorize or prohibit integration of locomotive control and train control functions. Should integration of these functions be allowed? If they are integrated, how should in-service failures of various kinds be handled (e.g., failure of one of two displays available to the engineer or failure of the conductor's display). If these functions are integrated, should the entire locomotive electronic system be subject to verification and validation under the new performance standards? If so, to what extent might train control functions be partitioned from other applications to simplify the problem, and in what way?

C. What Risk Assessment Methods Will Be Considered Adequate?

One of FRA's greater challenges concerning this proposed rule will be verification of compliance with the performance-based standard. The Standards Task Force has recommended an enforcement scheme under which railroads would conduct, when required, a risk assessment to show that the performance standard is met. In most cases, FRA envisions that the risk assessment will identify the assigned risk classes for the system, assign a numerical expression for each safety integrity level, specify a target failure rate, and identify the standards upon which the assessment and calculations were made. This information can be used as a basis to measure and identify the likelihood of a hazardous event and the potential for the system to function as intended. With this information, the railroad and FRA can confirm compliance with the performance standard.

The primary goal of the risk assessment required by this proposed 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. Most of the analytical techniques explored by the Standards Task Force analyzed relative risk levels much more effectively than they analyzed absolute risk levels. Thus, the proposed 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 they proposed creation of certain guidelines to be followed when conducting risk assessments. FRA feels 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 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. The proposed rule would allow 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. Initially, the Standards Task Force considered allowing only quantitative risk assessment methods 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. FRA invites comments addressing the extent to which qualitative risk assessment methods ought to be considered sufficient.

The Standards Task Force further recommended 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 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 proposes that risk assessment methods not meeting the guidelines of this proposed rule be allowed, so long as it could be demonstrated to 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 would retain authority to ultimately prevent implementation of a system whose Product Safety Plan does not adequately demonstrate compliance with the performance standard under the proposed 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 proposed 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 proposed 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 § 236.915(g)). Also, in such cases, FRA will be more likely to require an independent third party review and assessment (see § 236.915(h)).

Section-by-Section Analysis

Section 209.11 Request for Confidential Treatment

FRA proposes an amendment to this section, as recommended by the Standards Task Force, to clarify existing procedures for requesting confidential treatment for documents provided to the

FRA in connection with the agency's enforcement activities. First, the section would be amended 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. Second, the section would be amended to clarify the definition of what activities constitute FRA enforcement activities. Under the revised definition, enforcement would include receipt by the FRA of documents required to be submitted by FRA regulations, and all documents received by the FRA in connection with FRA's investigative and compliance activities, in addition to the development of violation reports and recommendations for prosecution.

Section 234.275 Processor-Based Systems

Section 234.275 proposes 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 feels it is 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 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). This focus captured the potential uses of Intelligent Transportation System (ITS) technology at highway-rail grade crossings. This proposed requirement 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) proposes 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 or that used in ITS, which 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). FRA is considering tailoring this definition to more accurately reflect the intent of the Standards Task Force, which was to include only technology not previously recognized for use in applications subject to part 234.

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

Paragraph (d)(1) is proposed to confirm that this section in no way authorizes deviation from the requirements of the 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.

Section 236.0 Application

As a general matter, this proposed rule would apply to all railroads, with two exceptions. First, railroads which operate on track wholly separate from 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 would be unaffected by the requirements of part 236. FRA proposes this change in 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).

Section 236.18 Software Management Control Plan

This section proposes a requirement for all railroads to 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 proposed requirement would provide 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 proposes this requirement because for a considerable time after the introduction of processor-based equipment into signaling systems, components of such systems were not always 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 driving to equipment locations, sometimes remote, these employees would even recklessly place PC boards and PROMs in tool bins and tool boxes. 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 Northeast Corridor (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.

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 would provide 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 would expect the software management control plan 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 cyclic redundancy check for verifying PROM contents. The Task Force had initially considered a requirement that railroads adopt configuration management plans, which would cover both software and hardware dealing with safety-critical aspects of processor-based signal and train control systems. Railroads expressed concern 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 invites comments specifically addressing this issue.

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.

This proposed requirement holds railroads 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. FRA invites comments specifically addressing this issue.

It is also recognized that this requirement may unduly burden the railroads in situations where they receive inaccurate information from the product manufacturer concerning manufacturer modifications. This poses safety risks because a railroad relying on a manufacturer's statement certifying compatibility, for example, with another manufacturer's system may create a dangerous situation if in fact the two products are not compatible. FRA feels that the railroads should be entitled to rely on the manufacturers' product information since manufacturers obviously know much more about the specifics of their products. In essence, the proposed requirement would impose a strict liability standard on the railroads regardless of culpability. FRA invites 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 further invites comments concerning the scope of a product manufacturer's duty to provide accurate information concerning initial software configuration of its products and any engineering control changes.

Paragraph (a) discusses the proposed application of this requirement to all railroads and how it applies to railroads not in operation as of the effective date of this rule. The Standards Task Force intended for this requirement to apply to all systems which would be specifically excluded by the § 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 allowance time for compliance was not covered by the Standards Task Force, FRA proposes a 24-month time period as sufficient. FRA welcomes comments specifically addressing this issue.

Paragraph (b) proposes a requirement for software management control plans, and further would require that the plan identify tests required by the system developer and/or the railroads in the event of replacement, modification, and disarrangement.

Section 236.110 Results of Tests

FRA proposes modification of 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 proposes to add two new sections to the list of sections to which § 236.110 applies: §§ 236.911 and 236.917(a), both of which apply 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) proposes to allow for electronic record keeping. In conjunction with FRA's policy of encouraging such methods where available and appropriate, FRA would like to allow for railroads to be able to avail themselves of this method. FRA proposes 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 offers changes to § 236.110 to make clear that records filed with a railroad supervisory officer with jurisdiction are subject to inspection and replication by FRA. 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 recordkeeping (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 proposed 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) proposes a requirement to specify the length of time records made in compliance with § 236.917(a) are to be kept. Paragraph (c)(1) proposes a requirement for all railroads to 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. For the following two reasons, the Standards Task Force recommended that these records be kept for one year, or until the next record is made. 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, the Task Force 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) proposes to allow electronic recordkeeping in lieu of preprinted paper forms.

Section 236.787a. Railroad

FRA proposes this definition to aid in standardizing the application provisions of its regulations. *See* also 49 CFR 238.5.

Section 236.901 Purpose and Scope

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

Section 236.903 Definitions

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 proposing 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.

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 remains the same from installation to installation; the design is not changed and it is not recompiled.

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 proposed 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 proposed rule offers standards in § 236.927.

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'' 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 invites comments addressing this issue specifically.

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 be 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 is considering amending the definition of predefined change to includes both

changes made directly to the product and changes to how the product is used. FRA urges parties developing product 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 hazard 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 Rules, Standards & Instructions (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.

The term ''product'' is proposed 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 the system itself, if processor-based. A processor-based subsystem is intended to signify a signal or train control system's subsystem which contains a processor-based component. A processor-based signal or train control system is intended to mean a signal or train control system which contains a processor-based component.

For issues related to the definition of ''risk assessment,'' please see major issue (c)-Risk Assessment Methods.

The term ''safety-critical'' is intended to apply to any function which must be correctly performed in order to avoid causing a hazardous condition to equipment or personnel. If not performing correctly, a safety-critical system, subsystem, or component could cause a hazardous condition or permit the occurrence of a hazardous condition which it was designed to prevent. 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 be 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 proposed definition ought to be modified to exclude references to what stages in a product's life cycle validation is performed. Commenters are invited to address this issue specifically.

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 recent rulemakings: FOX High Speed Rail Safety Standards, 62 FR 65478, Dec. 12, 1997; Passenger Train Emergency Preparedness, 63 FR 24630, May 4, 1998; and Passenger Equipment Safety Standards, 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 proposes that railroads implement FRA-approved system safety plans, enforce them, and update them as necessary. In this process, FRA proposes that the railroad 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) would require 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 proposed rule, FRA proposes that the railroad submit their 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 their initial RSPP to FRA. FRA believes that the RSPP must be used as a guide in the earliest conceptual stages of a project.

Paragraph (b) proposes that the RSPP address minimum requirements for development of 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).

Paragraph (b)(1) proposes a requirement 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 design for safety concerns are effectively identified and addressed at all stages of product development. FRA welcomes further comments concerning the railroad's claim and this distinction.

Paragraph (b)(2) discusses 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 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.

Paragraph (b)(3) proposes a requirement 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 proposed 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) discusses how the RSPP identifies configuration management requirements for the configuration of products subject to subpart H. The Standards Task Force felt this requirement was necessary to help railroads maintain consistency in the configuration management of the products they use.

Paragraph (c) describes the proposed 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 Docket Clerk, Office of Chief Counsel, for action by the FRA Associate Administrator for Safety. 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 (grant the petition, deny the petition, or request 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. Railroad members of the Standards Task Force suggested that FRA should notify them if an extension to the 180-day period will be needed, and provide the reasons therefore. FRA invites comments addressing FRA's handling of RSPP petitions beyond 180 days after filing. Paragraph (c)(4) proposes 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.

Paragraph (d) proposes 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) proposes a requirement 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) proposes 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. FRA notes that it may not be necessary to remit copies of the entire RSPP.

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 seeks comments on whether the elements contained in this section are adequate or whether there are other requirements that should be included to assure safety.

Paragraph (a)(1) would require 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 failsafe principle. FRA believes this provision is an important element that can be applied to determine whether safety is maximized and maintainability can be achieved. Railroads have expressed concern over the level of detail required in describing the product. Commenters are invited to address this issue.

Paragraph (a)(2) would require 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 invites comments addressing this issue.

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 would 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) proposes 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 justification provided 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. Interested parties are asked to comment on the adequacy of this process for preserving railroad safety.

Paragraph (a)(5) would require 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) proposes 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 on 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 the product (i.e., do not result in a hazard) would not be required to be recorded on the hazard log.

Paragraph (a)(7) would require that a risk assessment be included in the PSP. See major issue (c)-Risk Assessment Methods. FRA will use this information as a basis to confirm compliance with the minimum performance standard.

Paragraph (a)(8) proposes 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 absolutely that a product is 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 be 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.

Paragraph (a)(9) would also require that the PSP address safety verification and validation procedures. FRA believes verification and validation for safety are vital parts of the development of products and, in certain cases, should be performed by a third party. 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) would require 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 is considering consolidation of the concepts required in these two paragraphs.

Paragraph (a)(11) would require 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. The Standards Task Force felt this flexibility is necessary for designers to have.

Paragraph (a)(12) would require the railroad to include in its PSP the training, qualification, and designation program for workers who 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) would require 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 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) would require 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 were 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.

Paragraph (a)(16) would require warnings to ensure safety be 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 opposing 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) would require 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) would require 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, modifications, and 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) discusses 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) proposes a requirement 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 suggests 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) and invites comments addressing this issue.

Paragraph (b) discusses predefined changes. PSPs should 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) discusses incremental and maintenance changes. 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 changes 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.

Section 236.909 Minimum Performance Standard

FRA has attempted to craft 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 proposes 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) proposes 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 proposed standard places the burden on the railroad to demonstrate that the safety analysis provides a high degree of confidence. Under the proposed regulatory scheme, FRA will have access to the railroads' analyses, and will remain as likely to detect obvious shortcomings in them.

FRA is considering moving the second clause of the last sentence of paragraph (a), which requires the railroads to make available the necessary analyses and documentation. This requirement may be moved for organizational purposes to a more specific section in the proposed rule.

Paragraph (b) indicates that FRA would rely on the factors listed in § 236.915(g)(2) when assessing whether the petitioner made 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 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 invites comments specifically addressing this issue.

Paragraphs (c) and (d) propose 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 proposed scope for a full risk assessment. The Standards Task Force desired to clearly define the scope of the risk assessment by addressing only risks relevant to safety of the product. Thus, they decided that only affected risks need be addressed. Take, for instance, the risk of injury due to a broken handhold on a freight car. It is obvious that this risk 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 proposed 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) proposes 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. The Standards Task Force recommended allowing for 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 less) levels of risk exposure and severity for hazards associated with the previous condition. The Standards Task Force 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.

For changes analyzed using this simplified analysis, risk associated with operation under the new product is assumed to be proportional to its Mean Time to Hazardous Event (MTTHE). Therefore, changes in risk are assumed to be proportional to changes in MTTHE. The Standards Task Force proposed this simplified approach 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.

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 MTTHE is a sufficient indication of risk, thereby warranting a simplified risk assessment. The FRA seeks 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.

Paragraph (e) proposes general principles for the conduct of risk assessments and which methods may be used (see Major Issue (c)—''Risk Assessment Methods'').

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 earlier drafts the 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. Since most freight railroads keep safety data in terms of train-miles and gross train-miles for each railroad must be reported to FRA under part 225, FRA does not believe many railroads will burden themselves additionally by maintaining other data for purposes of this requirement.

The FRA seeks comment on this proposed requirement to account for exposure in the units mentioned above, specifically regarding the appropriateness of this approach and other possible approaches.

Paragraph (e)(2) also covers a proposed requirement for risk severity measurements. FRA proposes to allow 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 proposes 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 proposed 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 proposed performance standard in order for FRA to be able to effectively carry out its statutory duties as a regulatory agency. By proposing 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 proposes an allowance for railroads to use only fatality costs. 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, and/or operating speeds to be likely changes to accompany implementation of subpart H products. The proposal would require 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 will be 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 would 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 proposed requirement ensures that a minimum level of safety set by § 236.0, which would otherwise normally apply, 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 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). Since research in connection with the Corridor Risk Assessment Model indicates that operations in dark territory have a much higher risk of collision than in signal territory (when normalized on a train mile basis), this adjustment will set the safety baseline at an appropriate level for purpose of making the necessary comparison. 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.

FRA specifically invites comments addressing this method of accounting for concurrent changes in operating practices and comments proposing other methods.

Section 236.911 Exclusions

Paragraph (a) addresses the exclusion from the requirements of subpart H, or grandfathering, of existing products. 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.

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 the effective date of this subpart. The Standards Task Force felt these products ought to be excluded from the requirements of subpart H upon notification to FRA. FRA agrees that it would be too costly for the railroads and suppliers to redo 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, the Standards Task Force felt 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.

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 proven to provide a very high level of safety, reliability, and functionality. It would be a tremendous burden on the rail industry to apply subpart H to this proven technology. The Standards Task Force recommended 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. The Standards Task Force felt this would assure the safe performance of the system.

Paragraph (d) proposes requirements for modifications of excluded products. The Standards Task Force felt that 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.

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

Section 236.913 Notification to FRA of PSPs

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) proposes a requirement for preparation of a PSP, and discusses the circumstances under which a joint PSP must be prepared. ''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. FRA invites comments specifically addressing this issue.

In paragraph (b), FRA proposes 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, the Standards Task Force developed a matrix of railroad actions regarding processor-based signal and train control systems and what level of FRA scrutiny 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 ultimately recommended that existing processor-based train control systems should be subject to the requirements of proposed § 236.911, so the third situation was no longer considered as 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 recommendation, that review and approval is merited for all installations involving new or next-generation train control systems; mere informational filings will not be sufficient in this case. However, FRA invites comments specifically addressing this issue.

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 information filing at a minimum. Paragraph (b) also notes that some issues may be addressed through FRA's waiver process in part 211.

Paragraph (c) proposes 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 its 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 specify 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. Upon recommendation by the Standards Task Force, FRA has attempted to provide general criteria for situations in which FRA would require an informational filing to be upgraded to a full petition for approval. FRA proposes these filings will be upgraded only for good cause, and gives examples of what would be considered good cause. FRA invites comments specifically addressing these criteria for upgrading of informational filings.

Paragraph (d) discusses proposed 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 proposed rule, FRA does not require prior consultation but attempts to accommodate railroads' often tight development and implementation schedule 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, which is often a result of delayed government involvement. This proposed 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) discusses for 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) discusses 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. The Standards Task Force felt 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.

Paragraph (e)(1) proposes 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) proposes that FRA provide notice to the public of pending filings and petitions. This method of notice would 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) would allow for 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 would encourage 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 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 FRA will consider the product's compliance with recognized standards in product development. FRA feels the use of recognized standards in system design and safety analyses, accepted methods in risk estimates and proven safety records for proposed products would benefit their ability to act safely, consistently, and in a timely manner on PSP approvals. Paragraph (g)(2)(iii) states FRA will consider as a factor the overall complexity and novelty of the product design. Railroads have indicated this factor appears to be a barrier to innovation. FRA invites comments specifically addressing this topic. 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 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 has indicated its position with respect to the choice of risk assessment method in its discussion of entitled ''Major Issues (c)—Risk Assessment Methods.'' FRA specifically invites 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.

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 proposal 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) proposes factors considered by FRA when requiring a third party assessment and who qualifies as an independent third party.

Paragraph (h)(1) lists those factors, as developed by the Standards Task Force, many of which are the same used in deciding whether to approve a PSP. The Standards Task Force developed this list as 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 recommended by the Standards Task

Force. 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. Railroads have indicated concern that the proposed definition is unduly restrictive because it limits independent third parties to ones ''compensated by'' the railroad. 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 specifically invites comments addressing this issue.

Paragraph (h)(3) notes 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) discusses 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. The Standards Task Force agreed that a more informal process is warranted in order to alleviate safety concerns which are discovered after FRA is notified of the initial PSP. The Standards Task Force had considered a rule which would allow for all PSP amendments to be handled via informational filing, however, FRA felt the same concerns which apply to initial filing (either as a petition or as an informational filing) should apply to the PSP amendment.

Paragraph (j) discusses 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 they 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 proposes 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. Nonetheless, FRA invites comments specifically 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), are necessary in order for FRA to make informed decisions regarding the safety of testing operations.

Section 236.915 Implementation and Operation

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

Paragraph (a) proposes 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. 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 its 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 more to actual in-service performance than initial design safety considerations.

Paragraph (b) proposes a requirement that railroads will not exceed maximum volumes, speeds, or any other parameter limit or provision 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 invites comments specifically addressing this issue.

Paragraph (c) proposes 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 depends on the normal functioning of the system. This provision parallels current § 236.4, which applies to all devices. By proposing this paragraph, FRA merely intends to clarify that the standard in current § 236.4 applies to subpart H products.

Paragraph (d) proposes 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 proposes 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.

Paragraph (e) simply intends to convey that the standard in current § 236.11 would apply to subpart H products.

Section 236.917 Retention of Records

Paragraph (a) proposes the documents and records the railroad would be required to maintain at a designated office on the railroad for the life cycle of the product. All documents and records must be available for FRA inspection and copying during normal business hours. First, the railroad would need to maintain adequate documentation to demonstrate that the product PSP meets the safety requirements of the railroad's 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, would need to be kept for the life cycle of the product. Third, railroads would be 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 would require that implementation, maintenance, inspection, and testing records as described in § 236.907(a)(18)(ii) be recorded as prescribed in § 236.110.

Railroads have indicated that the product life cycle is too long a term to keep the data proving PSP compliance with the railroad's RSPP and training records. 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 invites comments specifically concerning this issue.

After the product is placed in service, paragraph (b) would require 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 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 preempt 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 that railroads take prompt countermeasures to reduce only the frequency of the safety-relevant hazard. 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 invites comments specifically addressing this issue.

Also, railroads have expressed concern 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 have proposed that they be given 30 days to report any inconsistencies. FRA is considering an allowance for railroads to fax or e-mail this report, 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 are invited to address this issue.

Section 236.919 Operations and Maintenance Manual

This section proposes 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. The Standards Task Force recognized it was necessary for railroad employees working with safety-critical products in the field to have complete and current information for installation, maintenance, repair, modification, inspection, and testing of the product being worked on. It was also suggested that this information be portable. As a result the Standards Task Force decided that this information be placed in a manual that could easily be carried into the field by the employee for use at the product work site.

Paragraph (a) works with §§ 236.905 and 236.907 and proposes 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 FRA.

Paragraph (b) proposes 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 proposes that plans identify the current version of software installed, revisions, and revision dates.

Paragraph (c) proposes that the Operations and Maintenance Manual identify the hardware, software, and firmware revisions in accordance with the configuration management requirements specified in the PSP. This proposed requirement is most easily understood in the context of the requirement for a configuration management control plan as specified in § 236.18.

Paragraph (d) proposes 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 for the railroads 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 railroad 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 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 is crucial

to maintain 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 the 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 roadway workers whose duties require knowledge and understanding of operating rules.

Paragraph (a) proposes 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.

Paragraph (b) proposes 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 employees and contractor's 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. 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 they were also assigned to perform those tasks.

The intent of this section is to ensure that employees who work with products, including contractors, know how to keep them operating safely. The proposed rule grants the railroad flexibility to focus and provide training that is needed in order to complete a specific task. However, this proposal is designed to prevent the railroad 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 contractors' 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 railroad will identify inspection, testing, maintenance, repairing, dispatching, and operating tasks for the equipment and develop written procedures for performance of same. Paragraph (a)(4) proposes that the railroad identify additional knowledge and skills above those required for basic job performance necessary to perform each task. Railroads have expressed concern regarding this requirement, and commenters are invited to address this issue.

Paragraph (a)(5) proposes that the railroad 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.

Paragraph (a)(6) proposes 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 they 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 they 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.

Paragraph (a)(7) proposes 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 employees and contractors' employees maintain the knowledge and skills necessary to safely perform their assigned tasks. Paragraph (a)(8) proposes a requirement to compare actual and desired success rates for the examination. Railroads have expressed concern about this particular requirement, and commenters are invited to address this issue.

Paragraph (b) conveys that in addition to the training of persons described in paragraph (a), the training program must require that only persons designated as qualified under the railroad's training program will be allowed to perform safety-related inspection, testing, maintenance, repairing, dispatching, or operating tasks. The railroad must maintain records which designate persons who are qualified to perform these tasks per the requirements of 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.

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 of instructions for control of trains and other on-track equipment when the advanced 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 proposes 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 invites comments addressing the issue of whether a formal definition is needed for ''other operating personnel.'' 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 that action or response ensures proper operation of the system and safe operation of the train.

Paragraph (b) notes 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) discusses requirements for use of a train control system to effect full automatic operation, as defined in § 236.903. FRA acknowledges that this proposed 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 proposed rule offers the standards in this paragraph.

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

Paragraph (c)(2) discusses required areas of skills maintenance training. In particular, this requirement recognizes the significance which the Standards Task Force placed on skills maintenance by manual starting and stopping of the train. Although manual starting and stopping, manual operation, and simulation training are all necessary to ensure effective maintenance of skills, the Standards Task Force felt that other options must be available. For instance, it may be burdensome for railroads, especially smaller operations, to offer simulator training to its locomotive engineers/operators. Thus, the Standards Task Force felt that in this instance training requirements can be worked out individually between the railroad, its labor representative and the FRA. In all cases, the PSP must define the appropriate training intervals for these tasks.

Section 236.929 Training Specific to Roadway Workers

This section would require 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.

Appendix B to Part 236—Risk Assessment Criteria

FRA proposes Appendix B as a set of criteria for performing risk assessments for products sought to be implemented on a railroad. During the Standards Task Force deliberations, 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 proposing a requirement that the risk assessment criteria be followed, but allowing for other criteria to be used if FRA agrees it is suitable. FRA feels this strategy adequately allows for the flexibility of a performance standard, yet offers concrete guidance on how a railroad or supplier can comply with the standard. As a practical matter, FRA believes that the overwhelming majority of risk assessments will seldom vary widely from the Appendix B criteria. FRA is aware of few known reasonable alternatives, and the criteria themselves are for the most part conventional, common sense methods of achieving the stated objectives.

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 train 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 proposed product, FRA is only interested in residual risks, or those which remain even after all mitigating measures have been taken.

Paragraph (b) discusses risks concerned 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) discusses how previous condition is computed. The proposed 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 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 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 quantitative MTTHE values may be difficult to assign. In these cases, FRA proposes allowing qualitative values to be used or estimated. Furthermore, for all human-machine interface components/subsystems, FRA proposes appropriate MTTHE estimates 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. Under the proposed rule, all MTTHE estimates must be made with a high degree of confidence, and must 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 did not provide any criteria as to how such a compliance process would be expected to operate, FRA invites comments addressing this issue.

Paragraph (g) proposes 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) proposes 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) discusses 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 proposes a requirement for documentation of assumptions. FRA envisions sampling and reviewing fundamental assumptions both prior to a product is implemented and after operation for some time. FRA intends for railroads to confirm the validity of initial risk assessment assumptions by comparing 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) proposes 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. However, if an unidentified fault path is discovered in service which leads to an previously unidentified safety-relevant hazard, then the threshold for defects in the PSP is automatically exceeded, and the railroad must take mitigating measures pursuant to proposed § 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 would require 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 would 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

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 as to how much safety can be achieved due to technology limitations, cost, and other constraints, and, upon recommendation from the Standards Task Force, proposes this appendix, recognizing this principle.

Paragraph (a) discusses the purpose of this appendix. Appendix C sets forth minimum criteria and processes for safety analyses conducted in support of RSPPs and PSPs.

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 they believe it does not apply. These safety considerations and principles resulted from early Standards Task Force meetings 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.

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 are.

Paragraph (b)(2) addresses design considerations dealing with systematic error. Systematic errors are those that can occur when the product is poorly developed and/or the human-machine interface is not given proper design attention.

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.

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 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 ''handshake'' in the design will determine whether received data is corrupted or not.

FRA is considering adding a separate paragraph 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.

Paragraph (c) proposes that certain listed standards be used for verification and validation procedures. These standards are already current industry/consensus standards and are more specifically describe the particular types of products.

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

Paragraph (a) discusses the purpose of an independent third party assessment of product validation and verification. FRA believes this requirement, as recommended by the Standards Task Force, is necessary for two primary reasons which became apparent through FRA's experience with earlier advanced signal and train control system projects.

By the early 1990's it was evident that technology could be fashioned to end the continuing series of collisions that plagued the railroad industry. The National Transportation Safety Board (NTSB) had studied 50 major rail collision incidents that NTSB determined could have been prevented had a system of positive train separation been in use. NTSB's recommendations for the need of a positive train separation system are given in its accident report titled ''Head on Collision Between Burlington Northern Railroad Freight Trains 602 and 603 near Ledger, Montana, on August 30, 1991'' (NTSB/RAR–93/01). However, it was also apparent that the railroad industry was not persuaded that such technology represented a sound investment in light of other capital needs.

The FRA Administrator held a series of round table discussions with members of industry to come up with ways to increase railway safety. Industry responded with the creation of various communications-based positive train separation and positive train control projects. Also during this time, under the New Generation High Speed program, 59 FR 46470 (September 8, 1994), the FRA initiated a new Incremental Train Control System (ITCS) train control system project in

Michigan. The ITCS project, known within Michigan DOT as the Mercury Project, is jointly funded by FRA, the State of Michigan, and Amtrak. Harmon Industries, the project supplier and builder, describes ITCS as a ''vital overlay'' system. This means that it utilizes the existing track circuits as part of its safety-critical communication-based system to allow higher train operating speeds, particularly at railroad crossings. As of the date of this printing, the first phase of the ITCS system is being tested in the Detroit-to-Chicago line in a 71-mile length of track between Kalamazoo and New Buffalo, Michigan.

Due to the novelty of the use of such complex technology in a railroad signal and train control application, FRA felt a validation and verification process, particularly for the software, was necessary to assure safety. FRA and Harmon agreed that Harmon should employ industry-accepted methods and procedures for safety validation and verification of their hardware and software. In addition, FRA felt that an independent third party should be involved in an assessment of the supplier's safety efforts. The necessity of an assessment was prompted by two concerns. First, FRA was concerned that some safety-related activities during development may be sacrificed in the event the supplier came under pressure to meet a project deadline. Second, a third party auditor often brings a variety of fresh ideas and methods to plug any unintended safety gaps.

FRA feels the ITCS concerns may apply to certain products developed under subpart H in order to ensure their safety integrity. This is particularly important when there are no safety records available on which FRA can assess a new product's reliability and endurance during operations. FRA feels an independent review will greatly enhance the safety of the systems and will ultimately work to the railroad's advantage. The Standards Task Force has recommended specific criteria for determining whether a third party assessment ought to be performed. 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 safety requirements 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, Preliminary Hazard Analysis (PHA) is performed in the design stage of a product. It attempts, in an early stage, to classify the severity of the hazards and to assign an integrity level requirement to each major function. PHA is part of the preliminary safety analysis, as required by the railroad's RSPP.

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. A small group of members from the PTC Working Group comprised the Human Factors Task Force. The task given them was to develop comprehensive design considerations for human factors and human-machine interfaces. This appendix outlines their efforts, which address 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 proposed 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 task force 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. HMIT 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 proposes to promote 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 proposed 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 proposed 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 render products that are safe and efficient.

Regulatory Impact

Executive Order 12866 and DOT Regulatory Policies and Procedures

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

FRA has prepared an Initial Regulatory Evaluation addressing the economic impact of the proposed 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, FRA, 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.

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 systems safety regulation is the provision of a safe operating environment for trains. The particular benefit of this proposed rule is the facilitation of introducing new technology into the field of signal and train control under minimal government scrutiny.

The proposed rule would regulate 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 proposed performance standard 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 proposes 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 proposed 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 proposed rule would ensure these alternatives are at least as safe as the current system. Thus, FRA envisions only one case where the proposed rule could possibly impose a situation not in the railroad's best interest. FRA does not believe this case would be a common occurrence.

The proposed 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 exceed 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. The primary cost of this proposed rule is the gathering of that 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 proposed 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 not feasible to conduct the currently required tests, and it is certainly less expensive to maintain a software management control plan. Thus, insofar as existing processor-based systems are concerned, the proposed rule would be less costly than the current rule, and FRA believes it would 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 would be, and when the benefits would occur. Because of the industry consensus involved (labor, management, and suppliers), FRA believes the benefits appear to outweigh the cost. The rule does not appear to have any effect of transferring costs from the railroads to the suppliers. Thus, FRA believes the railroads' assent appears to be based on genuine economics.

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

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 proposed rule should not have a significant economic impact on small entities. The proposed rule does not require the implementation of processor-based signal and train control systems, but merely proposes 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 proposed 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 further 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.

Paperwork Reduction Act

The information collection requirements in this proposed 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 responses	Average time per response	Total annual burden hours	Total annual burden cost
234.275—Processor Based Systems—Deviations from requirements.	100 Railroads	25 letters	2 hours	50 hours	$1,900
236.18—Software Management Control Plan.	100 Railroads	30 plans	20 hours	600 hours	22,800
236.905—Railroad Safety Program Plan (RSPP).	100 Railroads	10 plans	50 hours	500 hours	21,800
RSPP Modifications	100 Railroads	5 RSPP Mod.	20 hours	100 hours	4,360
236.907—Product Safety Plan (PSP)	100 Railroads	20 plans	80 hours	1,600 hours	60,800
236.909—Minimum Performance Standard—Petitions for Review and Approval.	100 Railroads	5 petitions	60 minutes	5 hours	330
Full Risk Assessment	100 Railroads	3 full assess	1,000 hours	3,000 hours	375,000
Abbreviated Risk Assessments	100 Railroads	16 abb. assess	80 hours	1,280 hours	160,000
Subsequent Years—Full Risk Assessments.	100 Railroads	5 amend docs	400 hours	2,000 hours	250,000
Subsequent Years—Abbreviated Risk Assess.	100 Railroads	5 amend docs	20 hours	100 hours	12,500
Alternative Risk Assessments	100 Railroads	3 documents	40 hours	120 hours	4,560
236.911—Exclusions—Notifications	100 Railroads	20 notifications	2 hours	40 hours	1,520
Additional Product Safety Pans (PSPs).	100 Railroads	2 plans	80 hours	160 hours	6,080
236.913—Notifications to FRA of PSPs.					
Informational Filings/Petitions for Approval.	100 Railroads	5 notifications	60 minutes	5 hours	190
Informational Filing—Add'l Info. Requested.	100 Railroads	32 filings	8 hours	256 hours	9,728
Additional Documents Requested/by FRA.	100 Railroads	10 data calls	8 hours	80 hours	3,040
Technical Consultations	100 Railroads	10 data calls	4 hours	40 hours	1,520
Petitions for Final Approval	100 Railroads	5 consultations	8 hours	40 hours	1,400
Additional Documents Requested by FRA.	100 Railroads	20 petitions	4 hours	80 hours	3,040
Further Consultations	100 Railroads	5 data calls	8 hours	40 hours	1,520
Other Petitions for Approval	100 Railroads	5 consultations	4 hours	20 hours	760
Additional Documents/Info. Requested.	100 Railroads	5 petitions	60 minutes	5 hours	190
236.917—Retention of Records	100 Railroads	22 documents	4 hours	88 hours	3,344
PSPs—Safety Hazards—Reporting Inconsistencies.	100 Railroads	80 reports	2 hours	160 hours	6,080
236.919—Operations and Maintenance Manual.	100 Railroads	25 manuals	4 hours	100 hours	3,800
Plans For Safety-Critical Products	100 Railroads	20 plans	40 hours	800 hours	30,400
Hardware/Software Revi. Documented in OMM.	100 Railroads	5 revisions	2 hours	10 hours	380
Identification of Safety-Critical Components.	100 Railroads	10,000 markng	1 minute	167 hours	4,843
236.921—Training Programs	100 Railroads	20 programs	80 hours	1,600 hours	60,800
Training Sessions—Railroad Employees.	100 Railroads	220 sessions	40 hours/20 hours	8,400 hours	1,050,000
236.923—Task Analysis/Basic Requirements—Records.	4,400 RR Employees.	4,400 records	10 minutes	733 hours	27,854

All estimates include the time for reviewing instructions, searching existing data sources, gathering or maintaining the needed data, and reviewing the information. Pursuant to 44 U.S.C. 3506(c)(2)(B), the FRA solicits comments concerning: whether these information collection requirements are necessary for the proper performance of the function of FRA, including whether the information has practical utility; the accuracy of FRA's estimates of the burden of the information collection requirements; the quality, utility, and clarity of the information to be collected; and whether the burden of collection of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology, may be minimized. For information or a copy of the paperwork package submitted to OMB contact Robert Brogan at (202) 493–6292.

FRA believes that soliciting public comment will promote its efforts to reduce the administrative and paperwork burdens associated with the collection of information mandated by Federal regulations. In summary, FRA reasons that comments received will advance three objectives: (i) Reduce reporting burdens; (ii) ensure that it organizes information collection requirements in a ''user friendly'' format to improve the use of such information; and (iii) accurately assess the resources expended to retrieve and produce information requested. *See* 44 U.S.C. 3501.

Comments must be received no later than October 9, 2001. Organizations and individuals desiring to submit comments on the collection of information requirements should direct them to Robert Brogan, Federal Railroad Administration, RRS–21, Mail Stop 17, 1120 Vermont Ave., NW., MS–17, Washington, DC 20590.

OMB is required to make a decision concerning the collection of information requirements contained in this proposed 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. The final rule will respond to any OMB or public comments on the information collection requirements contained in this proposal.

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**.

Environmental Impact

FRA has evaluated this proposed 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 proposed 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 proposed regulation and the conclusion that the proposed rule would not, if implemented, have a significant environmental impact.

Federalism Implications

This proposed rule has been analyzed in accordance with the principles and criteria contained in Executive Order 13132, and it has been determined that the proposed rule does not have sufficient federalism implications to warrant the preparation of a federalism summary impact statement. However, if it is determined through the comment period that federalism is impacted, FRA will document its consultations with State and local officials as appropriate and a federalism summary impact statement will be included in any final rule. FRA has consulted State and local officials in developing this proposed rule. The RSAC, which recommended this proposed rule, 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.

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 proposed 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.

Request for Public Comments

FRA proposes to amend parts 209, 234, and 236 of title 49, Code of Federal Regulations, as set forth below. FRA solicits comments on all aspects of the proposed rule whether through written submissions, participation in a public hearing, or both. FRA may make changes in the final rule based on comments received in response to this proposed rule.

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 Proposed Rule

In consideration of the foregoing, FRA proposes to amend chapter II of title 49, Code of Federal Regulations as follows:

PART 209—[AMENDED]

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

49 U.S.C. 20103, 20107, 20111, 20112, 20114, and 49 CFR 1.49.

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

(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:

49 U.S.C. 20103, 20107, and 49 CFR 1.49.

4. Add a new undesignated centerheading and new section 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 (date of final rule publication).

(c) The Product Safety Plan 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.

PART 236—[AMENDED]

5. Revise the authority citation to part 236 to read as follows:

Authority: 49 U.S.C. 20103, 20107, 20501–20505, and 49 CFR 1.49.

6. Amend § 236.0 to revise paragraphs (a) and (b), redesignate paragraph (f) as paragraph (g), and add new paragraph (f) to read as follows:

§ 236.0 Applicability.

(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.

* * * * *

(f) 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.

7. Add new § 236.18 to read as follows:

§ 236.18 Software management control plan.

(a) Within 24 months of (date 60 days after publication of final rule), each railroad shall adopt a software management control plan for signal and train control systems. Railroads commencing operations after (date 60 days after publication of final rule) shall adopt a software management control plan for signal and train control systems prior to commencing operations.

(b) 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 identify the tests required by the system developer and/or the railroads in the event of replacement, modification, and disarrangement.

8. 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.

(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 secure, is inaccessible to FRA or railroad employees requiring access to discharge their assigned duties, or fails to adequately track and monitor the equipment. In such case, FRA records such a determination in writing, includes a statement of the basis for such action, and provides a copy of the document to the affected railroad.

9. 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.

10. Add new subpart H to read as follows:

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

Sec.

236.901 Purpose and scope.
236.903 Definitions.
236.905 Railroad Safety Program Plan (RSPP).
236.907 Product Safety Plan (PSP).
236.909 Minimum performance standard.
236.911 Exclusions.
236.913 Notification to FRA of PSPs.
236.915 Implementation and operation.
236.917 Retention of records.
236.919 Operations and Maintenance Manual.
236.921 Training and qualification program, general.
236.923 Task analysis and basic requirements.
236.925 Training specific to control office personnel.
236.927 Training specific to locomotive engineers and other operating personnel.
236.929 Training specific to roadway workers.

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

§ 236.901 Purpose and scope.

(a) What is the purpose of this subpart?

The purpose of this subpart is to ensure the safe operation of trains using 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 satisfactorily explains:

(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 products in-use.

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 means that 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).

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 contains only: information relevant to determining the safety of the resulting system; information relevant to determining compliance with this part; and information 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)).

Preliminary Safety Analysis means the initial PSP analysis which results in a comprehensive listing of all safety functions that a system, subsystem, or component will perform. The analysis will insure that hazards are controlled when they occur, and that the risks associated with such hazards are either eliminated or mitigated prior to further development. (The initial product safety plan analysis methodology that provides a safety plan which regulates quality assurance, development, testing, implementation, and maintenance of each product.)

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 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

(1) Use of the product under all intended operating conditions or

(2) 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 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.

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 validation and verification methods for the preliminary safety analysis, initial development process and future incremental changes, including standards to be used in the validation and verification process, consistent with Appendix C to this part. The RSPP must require that a copy of any non-published standards be included with 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 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 modifications to be made, the reason for the modifications, and the effect of the modifications 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 validation and verification 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 Associate Administrator for Safety to be equally suitable;

(12) A complete description of the specific training 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-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, over 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 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.

(c) What requirements apply to other product changes? 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. Changes classified as maintenance require validation.

§ 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 make the determination, 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 determines sufficiency. 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? 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. This determination must be supported by credible safety analysis sufficient to persuade a reasonable decision-maker 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 (remote). An abbreviated risk assessment may be used in lieu of a full risk assessment to show compliance with the performance standard if:

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

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

(3) Exposure to such hazards does not change from 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 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 adjusted for exposure. Exposure must be expressed as total train miles (and, as applicable, total passenger miles) traveled per year. Severity 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 severity is measured strictly in terms of fatalities.

(3) If changes in the physical or operating conditions on the railroad are planned coincident with introduction of or within the expected life cycle of the product subject to review under this subpart, the previous condition shall be adjusted to reflect any associated impact on risk. 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 track and other changes required to support projected increases in train operations.

§ 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 (the date 60 days after publication of the final rule). 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 (date of publication of final rule) may be excluded upon notification to FRA by (60 days after date of publication of final rule) if placed in service by (3 years after date of publication of final rule). 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-based train-dispatching and/or central safety computer system.

(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 Notification to FRA 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 will be 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 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, and the PSP describes a locomotive-borne product that commingles safety-critical train control processing functions with locomotive operational functions. In addition, good cause would include 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 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 for 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 could include 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.

(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. 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–G of this part to the product that will not apply during testing;

(v) Date proposed testing to begin;

(vi) The location of the tests; and

(vii) Effect 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 § 236.917(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 for the life cycle of the product:

(i) 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;

(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.

(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 to the FRA Director, Office of Safety Assurance and Compliance, 1120 Vermont Ave., NW, Mail Stop 25, Washington, DC 20590, within 15 days of discovery;

(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.

(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 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? The railroad 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; and

(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.

(b) What competences are required? The railroad'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 railroad 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 the railroad's products. This will include 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 training (CBT), 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) and their direct supervisor(s) to successfully complete the 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 training (CBT), 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) Evaluate the effectiveness of the training program by comparing the desired success rate specified in § 236.923(a)(1) with the actual success rate.

(b) What training records are required? The railroad 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 available for inspection and replication by FRA.

§ 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.

11. Add new Appendices B–E to part 236 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 and/or component must be determined for the integrated hardware/software (where applicable) as a function of the Mean Times To Failure (MTTF) (expressed as failure laws), failure restoration rates, and the integrated hardware/software coverage of all processor-based subsystems and/or components. Train operating and movement rules, along with components that are layered in order to enhance safety-critical behavior, must also be considered. System safety-critical design for verification and validation documentation must support the risk-oriented assessment and validate the methodology used to arrive at the assessment results.

(f) How are processor-based subsystems/components assessed?

(1) An MTTHE value must be calculated for each processor-based subsystem and component, indicating the safety-critical behavior of the integrated hardware/software subsystem and/or component. The human factor impact must be included in the assessment, whenever applicable, to provide an integrated MTTHE value. The MTTHE calculation must consider the permanent and transient hardware failure rates (hardware, design and software coding errors), coverage of the integrated hardware/software (application, executive and input/output driver software) subsystem or component, phased-interval maintenance, and the restoration rates in response to 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 the permanent and transient hardware failure rates, phased interval maintenance and fault coverage of each non-processor-based subsystem or component and the restoration rate.

(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 Mean Time To Failure (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.

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 requirements were satisfied 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. The safety of the product in the normal operating modes must not depend upon the correctness of actions or procedures used by operating personnel. There must be no hazards that are categorized as unacceptable or undesirable. Hazards categorized as unacceptable must be eliminated by design.

(2) *Systematic failure.* The product must be shown to be free of unsafe systematic failure—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 and/or coding phases; human errors that could impact hardware design; unsafe conditions that could occur because of an improperly designed human-machine interface; installation and maintenance errors; and errors associated with making modifications.

(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, the system must restart itself without human intervention. 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 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 and/or software) 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 and/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 and/or electrostatic discharges;

(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 and/or software. 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.

(c) What standards are acceptable for verification and validation?

(1) The standards employed for verification and/or validation 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. All standards listed below must be the latest revision date 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 (July 1998) Railway Applications: Software for Railway Control and Protection Systems (draft);

(C) prENV50129: 1998 Railway Applications: Safety Related Electronic Systems for Signaling (draft); and

(D) EN50155 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 Manual of Recommended Signal Practices, Part 17 (this is an industry, rather than a consensus standard, and must bear the date of adoption).

(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.

(B) IEC 61508–2 (Ed. 1.0BBPUB, draft) Part 2: Requirements.

(C) IEC 61508–3 (1998–12) Part 3: Software requirements.

(D) IEC 61508–4 (1998–12) Part 4: Definitions and abbreviations.

(E) IEC 61508–5 (1998–12) Part 5: Examples of methods for the determination of safety integrity levels.

(F) IEC 61508–6 (Ed. 1.0BBPUB, draft) 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.

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 hardware or software failures (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 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.

Appendix E to this Part—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 and/or designs a system or subsystem 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 situation 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) Limited Memory. 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 ensure 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 for minimum resolution of visual displays;

(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 type and importance of relevant entities;

(iii) Understanding of the evolution of the situation over time;

(iv) Knowledge of 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 July 16, 2001.

Betty Monro,

Deputy Federal Railroad Administrator.

[FR Doc. 01–19428 Filed 8–9–01; 8:45 am]

BILLING CODE 4910–06–P