

Much Ado About Safety

Regulations, Standards and Recommended Practices

By Bill Petit

www.billpetit.com

This article was originally published in Railway Age in 2003.

Mr. Petit is Vice President of Technology for Safetran Systems. He has supported the RSAC process for its entire timeframe as a representative of the Railway Supply Institute (RSI), and has also been active in the development of consensus industry standards through AREMA and IEEE.

It seems like only yesterday that the Federal Railroad Administration (FRA) set out to develop regulations related to the safety of processor-based signal and train control systems. Actually, it was September of 1997 that the Railroad Safety Advisory Committee (RSAC) accepted the task of developing “standards for new control systems”. In the 6 years since then, close to 30 meetings around the country have been held by the task force assigned this task (and RSAC became more commonly known as Railroaders Seeing America Comprehensively). This article will review the current state of the proposed FRA rule as well as the efforts that have been done by industry-related professional organizations to assist in the application of the rule for Signal and Communication Professionals.

First, a disclaimer regarding the Notice of Proposed Rulemaking (NPRM) must be made. The NPRM was published in the Federal Register on August 10, 2001. Since then, meetings have been held to discuss some the remaining issues with the rule but there has been no official publication of any changes. While it is likely that the final rule will closely reflect the NPRM, there is no guarantee of this. Comments in this article reflect the current state of the NPRM and the author's interpretation of some of the discussions since then. Curious readers can read the complete NPRM as well as individual comments and meeting minutes contained in the FRA docket located at <http://dms.dot.gov>. (After entering the website, do a simple search for docket number 10160).

The NPRM reflects a substantial change in the FRA view of rulemaking as it moves toward the concept of performance based regulation. At the beginning of the process, FRA noted that the existing "Rules, Standards and Instructions (Part 236) take a performance-oriented approach at the functional level, although they most often reference older technology". After much discussion, the task force agreed that the basic tenet of the new rule was that new products must not degrade safety. While this basic concept was agreed to early, this led to the difficult topic of how do you prove that a new system does not degrade safety. The rule itself discusses the process for compiling the evidence of risk comparison capable of demonstrating "to a high level of confidence" that the new system does not degrade overall safety. It must be noted that this new rule (which will become subpart H of Part 236) addresses all processor-based signal and train control system, not just those considered under the term "PTC" for Positive Train Control systems. It does not exempt a railroad from compliance with Parts A-G of the existing

Part 236 except to the extent that a safety plan demonstrates why those requirements are unnecessary or addressed by some other means.

Under the rule, each railroad will be required to develop a Railroad Safety Program Plan that describes a railroads strategy for addressing hazards associated with operation of processor-based systems and products. Each individual processor-based system or product has its own comprehensive Product Safety Plan (PSP) associated with it and the RSPP (which must be formally approved by the FRA) establishes the minimum requirements for the PSP. As a minimum the RSPP must address the following areas:

- A description of procedures for risk assessment
- Identification of the safety assessment process
- Identification of the Verification and Validation Process for the design (and the NPRM contains an Appendix identifying safety criteria that must be considered as well as some acceptable published standards.
- A description of the process used to identify and address human factors issues related to the system (and an appendix is provided in the NPRM highlighting factors to consider).

After the FRA has approved the RSPP, the railroads are responsible for creating a comprehensive Product Safety Plan (PSP) for each product or system that falls under this subpart. Although referred to in the proposed rule as a plan, this document actually contains the complete proof of safety developed over the lifecycle of the product

development and installation. Although the railroad is responsible for the PSP, it is likely that the product or system supplier will provide substantial input toward its creation.

Following is a list of what must be included in the PSP.

- Complete description of the product
- Description of the railroad operation where it is to be applied, including items such as train movement density, gross tonnage, hazardous materials volume, railroad operating rules and operating speeds.
- Operational Concepts document including information flows.
- Comprehensive list of all safety functions provided by the product.
- Description of how the product architecture satisfies the safety requirements.
- Description of all safety-related hazards including maximum threshold limits for each hazard.
- Risk assessment (discussed in more detail later).
- Comprehensive list of hazards and their mitigation techniques
- Description of safety assessment and validation procedures describing how the safety areas covered in Appendix C are addressed directly, addressed using other safety criteria, or not applicable. Appendix C addresses areas such as systematic and random failures, common mode failures, use of closed loop principle, etc.
- Description of the safety assurance concepts used in design including assumptions and dependencies
- Human Factors Analysis. Appendix E of the NPRM provides Human Machine Interface (HMI) design criteria to minimize negative safety effects.

- Description of training necessary for installation, operation, inspection, testing, repair and modification
- Description of specific procedures and test equipment necessary for installation, operation, inspection, testing, repair and modification
- Analysis of Part 236 Subparts A through G and how they are satisfied directly, satisfied by an alternative method, or not applicable.
- Description of the security measures necessary for the product over its lifecycle.
- Description of warnings to be placed in Operations & Maintenance manuals or to be placed directly on equipment.
- Description of initial implementation test procedures.
- Description of post-implementation testing and monitoring procedures, including test intervals and required record keeping.
- Description of safety-critical assumptions regarding product availability including a description of all backup methods of operation
- Description of all incremental and pre-defined changes to the product.

PSP's are required for each product and/or system covered by this subpart. If more than one RR operates over the territory (and the method of operation will change), a joining PSP must be prepared by the operating railroads. PSP's related to new or next-generation train control systems require submission of a petition for approval to the FRA. All other PSP's require only an informational filing to the FRA and it must be submitted at least 180 days in advance of the product being used in revenue service. Within 60 days after

receipt, the FRA must acknowledge receipt. In addition, they may request further information, or notify the railroad that they must submit a petition for approval. Reasons for this additional petition requirement would be that the product uses safety practices outside generally accepted use in railroad products and systems, has a unique architecture, or commingles safety-critical train control with locomotive operational functions. The FRA will periodically publish a topic list in the Federal register including docket numbers for informational filings and petitions for approval.

Within the proposed rule, there are a number of factors identified that the Associate Administrator for Safety will consider in evaluating the PSP. These include

- Whether or not all required information has been submitted
- If the risk assessment demonstrates that the proposed product satisfies the minimum performance standard (i.e. is at least as safe as the existing product or system).
- The extent to which recognized standards have been utilized
- Availability of quantitative data
- Complexity of product or system and extent to which it deviates from design practices associated with previously established histories of safe operation
- Degree of rigor and precision associated with safety analysis
- Extent to which validation processes and testing has identified uncovered faults and whether those faults have been addressed

- Whether the risk assessment technique used for the previous condition (base case) was the same as for the proposed system.
- Whether an independent third party assessment was required or performed.
- The degree to which the new product or system is relied upon as the primary safety system for train operations.
- The degree to which the new product or system is overlaid upon and is independent of existing safety-critical rules, practices and systems that will remain in place.

The FRA may also require an independent third party assessment based upon consideration of the same factors listed above.

The major remaining factor to be considered is what is involved in a risk assessment. A little safety background is necessary to help understand the process. Traditional safety analysis focuses on identification and mitigation of hazards. Top-level hazards (e.g. two trains attempting to occupy the same space at the same time) are identified by looking at functional requirements, system application, expert knowledge, and through knowledge of similar products or systems. From these top-level hazards, additional hazards are identified through fault tree analysis, brainstorming and checklists developed through experience. These hazards are then analyzed for severity and probability and categorized according to their expected risk. Mil-Std 882C provides general guidance on this process and AREMA Manual Part 17.3.5 provides additional guidance specific to the railroad signal and train control environment. The risk categories include unacceptable,

undesirable, acceptable with review, and acceptable without review. Mitigations are then developed for each hazard in order to shift it from an unacceptable risk category to an acceptable one. Specific design mitigation techniques with analysis and verification methods provided in other AREMA manual parts (Section 17) and also in an Institute of Electrical and Electronic Engineers (IEEE) Standard related to verifying vital functions in processor-based systems used for rail transit control (IEEE Standard 1483-2000). IEEE Standard 1474.1-1999 identifies a similar safety assessment and verification process to be used for Communications Based Train Control systems used in rail transit.

Under the proposed rule, the FRA allows two types of risk assessments to be performed. An abbreviated risk assessment for products and systems performing the same function as in the previous (or base case) condition is allowed. One interpretation of this would be that replacing an interlocking controller (either relay-based or a previous generation processor-based system) with a processor-based interlocking controller would qualify for this abbreviated risk assessment. This abbreviated risk assessment may be used only if

- No new hazards are introduced as a result of the change
- Severity of existing hazards is not increased from the previous condition AND
- Exposure to existing hazards does not increase from previous condition.

For the abbreviated risk assessment, the FRA requires that the Mean Time To Hazardous Events (MTTHE) for the new product is greater than the MTTHE for the previous condition. Of course, this must be supported by a credible safety analysis consisting of

both qualitative and quantitative portions. Although not published in the NPRM, it has been suggested to the FRA that the final rule contain a clause accepting products meeting the MTTHE recommendations contained in AREMA Manual Part 17.5.3 (providing that the product is developed in accordance with the other AREMA Part 17 recommendations and considering the safety criteria contained in Appendix C of the proposed rule). This proposal was accepted by the RSAC task force members and hopefully will provide detailed guidance for the abbreviated risk assessment.

A second risk assessment, known as a full risk assessment, is needed for Products and Systems not qualified for the abbreviated risk assessment. The full risk assessment adds train exposure as an additional factor to be considered. Full risk assessment identifies the accumulated risk of a train system in operation over a lifecycle of 25 years or greater. In essence, this assessment takes the hazard rate discussed above and overlays the railroad operations on top of it. In this case, the hazard must occur at the same time as a train is present at the hazard location, assuming the hazard would then be identified prior to the next train arriving. The risk can be expressed in terms of total accident costs (including property damage, injuries and fatalities) or it may be expressed strictly in terms of fatalities. In either case, the risk per million train miles for the proposed system must not be worse than the current risk per million train miles for the existing system. If changes in the current operations are changed as a result of introducing the new system, the “base case” risk assessment may have to be modified. Task force teams are still trying to work out the requirements for changing the base case assessment.

Full risk assessments require taking the following operating parameters into account along with the hazards identified through the traditional safety process described above.

- Track plan infrastructure
- Total number of trains and movement density
- Train movement operational rules, as enforced by the dispatcher and train crew behaviors (including human reliability assessment)
- Wayside subsystems and components
- Onboard subsystems and components

Other sections of the NPRM address slightly different topics and should be noted. One such requirement is for a software management control plan to be adopted within 24 months of rule publication covering all processor-based signal and train control systems, even those currently in revenue service. Another requirement is proposed for Part 234 noting that the requirements of this proposed subpart (236 H) are also applicable to highway-rail grade crossing warning systems containing new or novel technology, or providing safety-critical data to a railroad signal system.

This proposed rule marks a substantial departure from traditional FRA rules regarding signal and train control systems. It has the potential to more easily allow justification of technologies that may improve the overall safety of railroad operations. Suppliers of existing processor-based systems have spent many years developing and refining the safety techniques for using processors and have achieved an excellent safety record.

Many of the safety-related aspects of the NPRM come from practices already widely used in the industry. With new suppliers entering the market, this rule (and compliance with industry standards) should allow railroads to have confidence that the same level of safety will be maintained.

However, there are also unknowns as substantial areas of the rule will be subject to interpretation. Suppliers of systems built according to traditional safety assessment techniques are concerned that the additional risk assessment requirement (i.e. requiring hazards to be linked to operational exposure rather than focusing solely on hazard elimination as is generally done now) may add a substantial cost burden. Interpretation of some European standards, including requirements for third party assessment, has demonstrated this additional cost. This rule also imposes a burden on the FRA, as they will now have to provide substantial review of both system safety analysis and the detailed design of processor-based systems, areas that they have never addressed before. In order to support this need, FRA has already hired two staff members responsible for providing guidance in the area of safety-critical processor-based designs.

Assuming this rule is eventually published as written, it will be a major stepping-stone in FRA's involvement in processor-based designs. As long as all parties continue to work together as they have to date, reasonable interpretations can be made and the railroads will continue to benefit from the positive aspects of processor-based signal and train control systems.