

Bill Petit

www.billpetit.com

This editorial was originally published in Railway Age in 2005.

Most of the attention on the new FRA rulemaking for safety of processor-based train control (Part 236 subpart H) has focused on how it will apply to future positive train control systems. However, we shouldn't lose sight of the fact that this rule applies to all processor-based signal and train control systems. In this article, we'll take a look at what effects the rule may have on these existing systems (including next generation version of these systems), both from the perspective of what opportunities this will present, as well as what additional costs may be incurred. (Naturally, these are my opinions and I am not speaking on behalf of the FRA and their future interpretation of this rule.)

When the Rail Safety Advisory Committee (RSAC) initially undertook the development of this rule back in 1997, it was intended to be limited to Positive Train Control systems. During the ensuing working group meetings, it was decided to expand the rule coverage to all processor-based signal and train control products (and systems). The stated goal of the new rule is to assure that processor based signal and train control systems are at least as safe as the systems they are replacing. The rule allows this goal to be verified by either a full risk assessment or an abbreviated risk assessment. Next generation products performing conventional signal and train control functions (e.g. products compliant with Part 236 subparts A-G, such as interlockings, track circuits and cab signal systems) can be accepted for use through the use of an abbreviated risk assessment. This abbreviated

risk process allows the railroads Product Safety Plan (PSP) to demonstrate that the products have been developed in accordance with AREMA Manual Part 17 and Appendix C of the new rule. Basically this means that the products will continue to be built to the high standards of safety used for safety-critical processor-based systems today.

For products that wish to take advantage of technology to achieve compliance with parts A-G in a different manner, a full risk assessment is required to demonstrate that safety is not being compromised. This full risk assessment must compare the new operation to the previous case over at least a 25-year lifecycle. Included in the risk assessment are track plan infrastructure, total number of trains and movement density, train movement operational rules, wayside and onboard subsystems and human reliability assessments.

As a way of considering opportunities for railroads to reduce operating costs while maintaining (or increasing) the level of safety, lets consider a simple example. Existing 236 parts require periodic testing to verify that time locking is operational at interlockings. (Time locking is used to prevent canceling a signal, then clearing an conflicting route without allowing time for a train currently approaching the now cancelled signal to stop). These rules were originally intended to address relay based systems where it was possible to have shorted or grounded cables that may have affected operational issues, or where electro-mechanical components properties change over time (e.g. timing capacitors). Modern processor-based systems have continuously running internal self-checking mechanisms to verify that the operational logic and timing remains

the same. In addition, modern processor-based systems also allow operations to be monitored and verified during every train movement that exercised the logic. Therefore periodic testing of this time locking function is not necessary.

Even though the time locking function is verified using alternative methods, current FRA rules still require periodic testing requiring manpower and access to the railroad, thus interfering with operations. With subpart H, a process is identified allowing the railroad to demonstrate via a full risk assessment that the alternative approach is at least as safe as the current periodic testing that is required.

Since I'm not a believer in the proverbial free lunches, we'll now address some of the potential costs that railroads may incur in taking advantage of the new rule. Existing suppliers already adhere to the safety principles identified in this rule, and have been involved over the years with railroads, consultants and transit agencies to develop industry standards and recommended practices for safety design and assessment. These safety practices and analyses add overhead to the development costs for new products but are already in place today for existing suppliers. Additional work will be required by this rule to address risk comparison (including human reliability) and to formalize processes specifically to meet documentation requirements of the new rule. For the simple time locking example described earlier, we can assume worst-case operations (i.e. train density, etc) and complete a full risk analysis that is applicable anywhere on the railroad. However, the completion of this risk analysis will add cost to the railroad. Should the FRA require a third party review, costs will increase substantially.

In general, railroads will also incur the additional cost of creating and maintaining the Railroad Safety Program Plan (RSPP) required to be approved by the FRA, as well as the individual Product Safety Plans required for each new safety-critical processor-based product. RR's will also face additional costs for maintaining their training policies as well as formal policies for installation, periodic testing, maintenance, repair, as part of their internal quality control system and in a format allowing FRA to monitor the railroads compliance with their own system.