Performance Standards for Processor-Based Signal and Train Control Systems

Cynthia Walters

Grady Cothen

Railroad Safety Advisory Committee

May 29, 2002

PTC Comments and Resolutions

- This presentation will briefly describe comments to the NPRM and the resolutions provided by the PTC Working Group.
- Overview:
  - General issues
  - Comments by Rule Section
  - Major unresolved issue
  - Next steps

Responsibility

- Who is responsible, railroads or suppliers?
- Railroads responsible for systems as deployed
- [Suppliers implicitly responsible for their representations]

Sample Documents

- Will FRA provide sample documents (RSPP, PSP)?

- No, don't want to fall into "boilerplate" habit, but…
- NAJPTC will yield examples

NOTE: Propose to maintain the working group as a continuing forum; may address needs as they appear

Section 209.11 Request for Confidential Treatment

- Certain information submitted in required filings that railroads and suppliers may want protected.
- Some feel all safety info. should be public.
- FRA will protect info. appropriately categorized as confidential, but if challenged, courts make final decision. (see trade secrets handout)

Section 236.18 - Software Management Control Plan

- Concern that the allotted 24 months may not be sufficient to devise a software management control program for products already being designed
- Resolution - Rule text revised to allow total period of 30 months for full implementation which extends the 24 month period by 6 months.

Section 236.18 (cont.)

- Concern - Software plan should i.d. the process for ensuring proper configuration, not simply i.d. the tests.
- Resolution - Rule text revised so that plan requires description of process ensuring proper configuration.

Section 236.903 Definitions

- Proposed Definition of term “Train Control”
- Revision to the preamble to explain concept, but no attempt to craft a new definition.

Definitions (cont.)

- Term “High Degree of Confidence”
- Revised to apply only at the aggregate level and removed the word “remote”
- Term “Mean Time To Hazardous Event”
- No revision, explanation why group decided not to use MTBHE

Definitions (Cont.)

- Term “Validation” use IEEE definition.
- No revisions

Section 236.905 Railroad Safety Program Plan

- Concern - Information requested does not reside with the railroad.
- Concern – Confusion between risk assessment and safety assessment.
- Resolution - Railroads remain responsible.
- No group consensus on clarifying language, discussion of concepts added to section-by-section analysis.

Section 236.905 (cont.)

- Concern – Can internal suppliers processes for V&V be exempt from this requirement?
- Resolution – Rule Text revised to indicate non-published standards must be referenced (in lieu of providing standard w/filing)

Section 236.905(cont.)

- Concern – Allowing petitions to remain pending beyond 180 days will delay implementation.
- Resolution - No change in rule text. Rarely used. Explanation provided in section-by-section analysis.

Section 236.907 Product Safety Plan

- Concern that the list of railroad operating characteristics may not apply to each product.
- No revision in rule text. Section by section requires a simple explanation that a certain characteristic does not apply and why.

Section 236.907 (cont.)

- Concern that hazard log and hazard mitigation analysis should be included in the same document.
- Suggestion to use MIL-STD-882 classifications.
- No revision in rule text. FRA will not create templates for submissions.
- Objections in group, no rule text change.

Section 236.907(cont.)

- Suggestion that the concept of security be refined to mean formal methods.
- No rule text change. Concerned with all dimensions of safety.

Section 236.909 Minimum Performance Standard

- Concern - Use of term “High Degree of Confidence” too subjective.
- Concern – Level of proof necessary for abbreviated risk assessment.
- Resolution – No change in rule text account no acceptable substitute available.
- Resolution - No change in rule text. FRA’s expectations explained in section by section.

Section 236.909(cont.)

- Concern – Flexibility in use of risk parameters (train miles, hours of exposure, MIL-STD-882)
- No change in rule text. Use train miles.

Section 236.911 Exclusions

- Concern – Existing Solid State Equipment should not be grandfathered.
- Concern – Should product modifications caused by implementation details be included?
- No change to rule text: good track record, and extremely burdensome to subject to Subpart H requirements.
- Working group not able to craft more precise standard

Section 236.911(cont.)

- Concern – Products w/proven track record in other industries (including rail transit)?
- No acceptance by working group
- FRA to review and consider

Section 236.911(cont.)

- Post-meeting comment: systems with track record on international railways should be subject to exclusion (request for clarification affirming interpretation)
- FRA has issue under review; typically this kind of language applies to subject matter in service under FRA jurisdiction

Section 236.913 Notification to FRA of PSPs

- Who is responsible for submitting PSP under various scenarios? Is the PSP Portable?

- No rule text change but explanation provided in section-by-section:
- PSP's can be portable where one railroad anticipates using in several locations, ***OR***
- If supplier develops system under broad conditions of operation and one PSP can be adapted for use by different RRs.

Section 236.913 (cont.)

- Suggestion to allow conditional approval or shorter approval periods for less complex products.
- No change in rule text, but FRA suggests in section-by-section railroads notify agency of business-relevant dates and agency will attempt to accommodate.

Sections 236.921 – 236.929 Training Provisions

- Suggestion that FRA allow electronic record keeping.
- Concerns regarding the training of direct supervisors.
- Agreed; means of approval under review at FRA.
- Changed rule text to clarify that direct supervisors should be trained to handle to appropriately supervise.

Training (cont.)

- Concerns regarding maintenance of training records.
- Clarification in section by section that employer responsible for records of its own employees, but FRA will expect access to the appropriate records of contractors. RR ultimately responsible.

Training (cont.)

- Concern that training is product specific.
- Concern that supplier personnel should not need training.
- Task analysis will dictate. No rule text changed.
- Task analysis will dictate. If supplier personnel are performing certain functions, may need training.

Training (cont.)

- Suggestion to add language for training of roadway workers in case of abnormal operations.
- Rule text revised to reflect this comment.

Appendices C and D

- Appendix C (Safety Assurance Criteria – includes reference standards)
- Appendix D (Independent Third Party Review of Verification and Validation)
- Small team formed to recommend changes to Appendix C and D
- Team recommended following revisions:
  - Clarify appendices contain objectives not requirements.
  - Revised language addressing human error.

Appendices C and D (cont.)

- Revised language addressing mitigation of unsafe failures.
- Revised language addressing automatic restart of system.
- Revised language addressing single point failures. Revised language addressing unacceptable hazards.
- No changes for Appendix D.

Outstanding Unresolved Issue: Determining the Base Case

- Section 236.909 – Performance Standard
- New system at least as safe as old system (no degradation in safety)

Base Case (Cont.)

- Comment to NPRM raised issue addressing the system to be replaced, “base case” or “previous condition”.
- NPRM would require “adjustment” of the base case where changes in infrastructure and operations are planned.

Base Case (cont.)

- Performance better than existing rules require would be captured where existing infrastructure and operations will not change (and no adjustment is required).
- This is not necessarily “best” practice, but it may be.
- No way of capturing existing best practice in cases requiring “adjustment” was spelled out in NPRM.

Base Case (cont.)

- Commenter noted that actual capabilities of best current technology often exceed existing minimum standards, so--
  - Comparing new system w/min. standard may reduce safety.
  - Actual functioning of best available technology (compliant with present Part 236 should be part of the base case analysis).
- Working group did not concur.

Base Case (cont.)

- Working Group critique:
  - Concern with ratcheting of standard as traditional technology continues to improve.
  - Viewed as not consistent with philosophy of proposed rule.
- Possible rationale for rejecting comment: railroads are likely to exceed minimum standards under revised rules, just as they do today.

Base Case (cont.)

- FRA staff inclined to agree that the “best practices” concept, while it has merit, could introduce complexity and cause unexpected results.
- Still, the concept may have potential continued applicability for train control in support of higher speed operations, as discussed prior to NPRM.
  - Public agencies are the investors / should seek best practices where possible.

Base Case (cont'd)

- ***However,*** major party also made removing the requirement to adjust the base case a condition for consensus, except as necessitated by section 236.0.
- That is, no change would be made for future traffic density increases, changes in infrastructure, or increases in train velocity (except for 236.0 triggers).
- In FRA's view, this would be a step back from the NPRM.

Base Case Discussion

- Two issues: technical practicability and safety.
- Background concepts:
- Risk = probability x severity.
- Risk metric = societal loss per million train miles and per million passenger miles.

Base Case Discussion

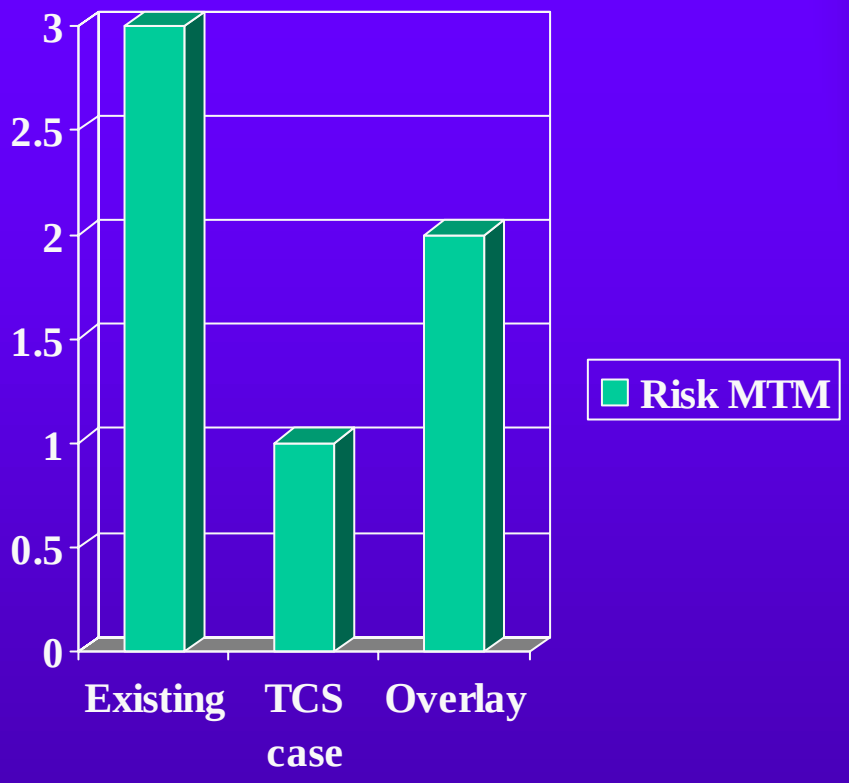
- Premise: strength of risk assessment is in comparing two scenarios with similarities and dissimilarities.
- Corollary: the more salient dissimilarities, the weaker the analysis.
- Major uncertainty in any S&TC analysis: likely ***severity*** of rare events.
- Inherent uncertainty in risk assessment exacerbates problem.

Note for following examples: values are purely arbitrary and provided as illustrations.

Base Case Discussion—Safety Concern Example

- Assume existing dark territory, 49 mph
- Density optimizes risk

  (Compare)
- Non-vital CBTC overlay would support more trains (line capacity); add passing sidings, turnouts
- Current alternative: TCS or dilute operating rules



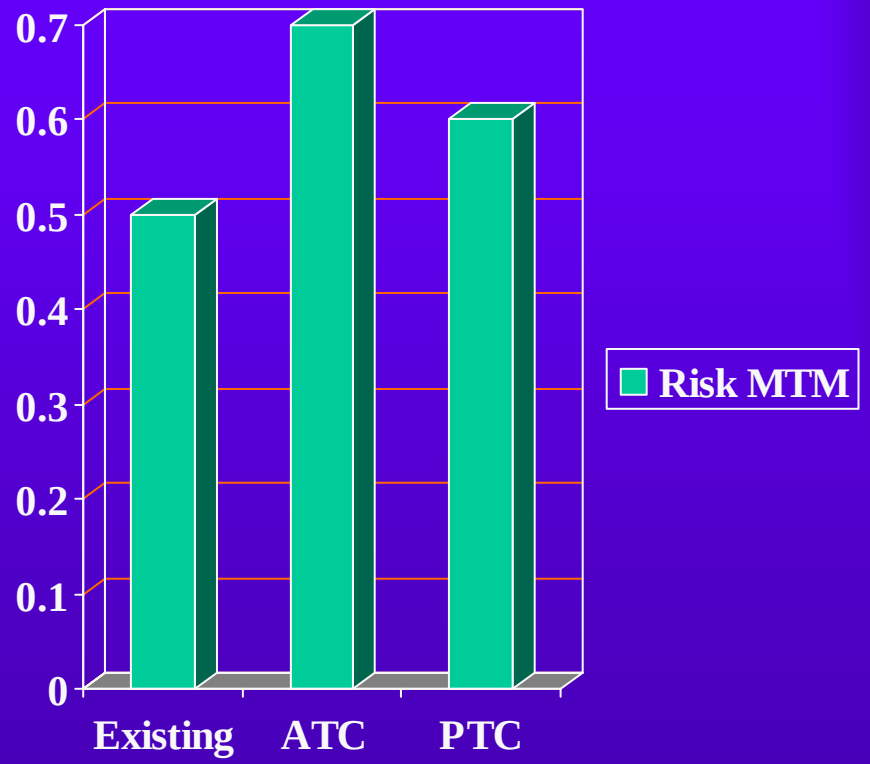
Base Case Discussion—Safety Concern Example

- In the example above, failure to adjust as necessary for planned density would allow traffic growth without full compensation for increased risk, including collisions and broken rail derailments.
- Benefits that have accrued from signalization could cease.
- It's true, FRA does not presently require TCS, but that's because it is needed for business reasons—***obviating the need*** for an FRA mandate.

Base Case Discussion -- Technical Practicality Example

- Low existing risk
- Dark territory, 25 mph (low severity)
- Density very low (2 trains daily)

  --(Compare)--
- New PTC system; support high-speed passenger rail and intermodal trains – some unequipped
- Rebuilt railroad, straighten curves, add sidings
- Current alternative: TCS/ACS/ATC with all trains equipped



Base Case Discussion -- Technical Practicality Example

- Because the new operating system will be nothing like the old one, any comparisons will be speculative.
- The low level of risk in the existing system will become an unrealistically low ceiling on the new operation, even though…
- Under present regulations and technology, the risk would be very acceptable.

Base case (cont.)

- Need to achieve consensus to move forward with a performance-based standard
- Resolving risk assessment issues central to having confidence in appropriateness of approach
- FRA is working with the parties to resolve this remaining issue – provided examples and explanatory material

Next Steps

- Resolve base case issue within the next month, including PTC Working Group approval
- Provide matrix with proposed issue resolution to full RSAC for approval by mail ballot
- Issue final rule
- Continue development of risk assessment guidance material in concert with Working Group