U.S. Department of Transportation
Federal Railroad Administration

PTC System Certification

PTC Safety Plan Prerequisites, Preparation, Content, Supporting Data and Review Process

Federal Railroad Administration – Positive Train Control (PTC) Symposium #3

August 20, 2018

Outline

1. Statute & Regulations Requiring PTC System Certification
2. Conditionally Certified Systems – Statistics
3. Lessons Learned – Why Improvements Are Needed
4. Baselining PTC Systems
5. FRA PTC Safety Plan Review Process

Section 1:
Statute & Regulations

Statute

The statute, codified at Title 49 United States Code (U.S.C.) § 20157, provides:

- The Secretary shall not permit the installation of any PTC system or component in revenue service unless the Secretary has **certified** that any such system or component has been approved through the approval process set forth in part 236 of title 49, Code of Federal Regulations, and complies with the requirements of that part.
    - Certification of PTC systems has been delegated to the FRA Associate Administrator for Railroad Safety and Chief Safety Officer.

Prior to PTC System Certification (but not *replacing* the requirement for certification):

- FRA may authorize a railroad to commence revenue service demonstration (RSD) under 49 CFR § 236.1035 (field testing requirements) or provisional operations in revenue service under 49 U.S.C. § 20157(h)(2) "to the extent necessary to enable the safe implementation and operation of a [PTC] system in phases."

Regulations

The regulations under 49 CFR part 236, subpart I define:

- **Who Must Obtain PTC System Certification** – *A host railroad*
- **How To Submit for PTC System Certification** – *PTC Safety Plan (PTCSP)*
- **What a PTCSP Must Include** – *Document the analysis of safety as a Non-vital Overlay, Vital Overlay, Stand-Alone or Mixed PTC system and provide the required documentation listed in 49 CFR § 236.1009(d) and, in detail, § 236.1015*
- **What Does PTC System Certification Mean** – *The system complies with the requirements of subpart I*

Regulations

Non-vital Overlay

Non-vital Overlay:

- A PTC system proposed as an overlay on the existing method of operation and *not* built in accordance with the safety assurance principles set forth in Appendix C to 49 CFR part 236
- Must be shown to:
  - Reliably execute the functions set forth in § 236.1005
  - Obtain at least 80 percent reduction of the risk associated with accidents preventable by the functions set forth in § 236.1005
    - When all effects of the change associated with the PTC system are taken into account
    - The supporting risk assessment shall evaluate all intended changes in railroad operations coincident with the introduction of the new system
  - Maintain a level of safety for each subsequent system modification that is equal to or greater than the level of safety for the previous PTC systems

Certified Non-vital Overlay PTC Systems:

- Interoperable Electronic Train Management System (I-ETMS)

Regulations

Vital Overlay

Vital Overlay:

- A PTC system proposed on a newly constructed track or as an overlay on the existing method of operation and built in accordance with the safety assurance principles set forth in Appendix C to 49 CFR part 236
- Must be shown to:
  - Reliably execute the functions set forth in § 236.1005
  - Have sufficient documentation to demonstrate that the PTC system, as built, fulfills the safety assurance principles set forth in Appendix C to 49 CFR part 236
    - The supporting risk assessment may be abbreviated as that term is used in subpart H of part 236

Certified Vital Overlay PTC Systems:

- Advanced Civil Speed Enforcement System II (ACSES II)
- Incremental Train Control System (ITCS)

Regulations

Stand-alone and Mixed Systems

Stand-alone System:

- A PTC system proposed on a newly constructed track, an existing track for which no signal system exists, as a replacement for an existing signal or train control system, or otherwise to replace or materially modify the existing method of operation
- Reliably execute the functions set forth in § 236.1005 and be demonstrated to do so to FRA's satisfaction
- Have a PTCSP establishing, with a high degree of confidence, that the system will not introduce new hazards that have not been mitigated
  - The supporting risk assessment shall evaluate all intended changes in railroad operations in relation to the introduction of the new system and shall examine in detail the direct and indirect effects of all changes in the method of operations

Mixed System:

- If a PTC system combining overlay, stand-alone, vital, or non-vital characteristics is proposed, the railroad shall confer with the Associate Administrator regarding appropriate structuring of the safety case and analysis

Regulations

Host Railroad Requirements:

- Before placing a PTC system in service, the host railroad must submit to FRA a PTCSP and receive PTC System Certification

- FRA approves the PTCSP and issues a PTC System Certification if FRA finds that the PTCSP and supporting documentation demonstrates that the system complies with 49 CFR part 236, subpart I

- Receipt of a PTC System Certification affirms that the PTC system has been reviewed and approved by FRA in accordance with, and meets the requirements of, subpart I

Regulations

- A PTCSP may reference and utilize any Type Approval previously issued by FRA to any railroad, provided that the host railroad:
  - Maintains a continually updated PTC Product Vendor List (PTCPVL) pursuant to § 236.1023
  - Shows that the supplier from which they are procuring the PTC system has established and can maintain a quality control system for PTC system design and manufacturing acceptable to the FRA Associate Administrator
  - The quality control system must include the process for the product supplier or vendor to promptly and thoroughly report any safety-relevant failure and previously unidentified hazards to each railroad using the product
  - Provides the applicable licensing information

Regulations

A PTCSP Shall:

- Include the FRA-approved PTCDP or, if applicable, the FRA-issued Type Approval
- Specifically and rigorously document each variance to the PTCDP or Type Approval, including the significance of each variance between the PTC system and its applicable operating conditions – or attest that there are no variances
- Attest that the system was built in accordance with the applicable PTCDP and PTCSP and achieves the level of safety represented
- May incorporate the PTCDP by reference, with the exception that a final human factors analysis shall be provided in the PTCSP (if the PTCDP has been previously approved)
- Include, as described in detail under 49 CFR § 236.1015(d), a:
  - Hazard log
  - Risk assessment of the as-built PTC system
  - Hazard mitigation analysis
  - Emergency and planned maintenance temporary rerouting plan
  - Documents and information required under § 236.1007 (add'l requirements for high-speed service) and § 236.1033 (communications and security requirements)
  - List of each location where a locomotive with a failed onboard PTC apparatus will be regularly exchanged or repaired, which must be the next forward designated location

Regulations

A PTCSP Shall:

- Also include a **description of**:
  - Safety assurance processes
  - Safety assessment and V&V processes, results, and whether or not the processes address safety principles in Appendix C (in whole, in part, or not at all)
  - Training plan for employees and contractors (see 49 CFR §§ 236.1041–1049)
  - Test procedures and equipment to ensure safe installation, operation, maintenance, repair, inspection, testing, and modification of the PTC system
  - Any additional warnings to be placed in the OMM and all warning labels
  - Configuration or revision control measures to ensure a railroad or its contractor does not adversely affect safety-functional requirements
  - How the PTC system will enforce all integrated hazard detectors
  - Initial implementation test procedures and all post-implementation testing and monitoring procedures (including intervals) necessary to establish safety-functional requirements are met and safety-critical hazards are mitigated
  - Each record associated with periodic maintenance, inspections, test, adjustments, repairs, or replacements and the system's resulting conditions
  - Safety analysis to determine if any risk remains of an unintended incursion into a roadway work zone due to human error
  - Any alternative arrangements for 1005(a)(1)(i)
  - How the PTC system will enforce authorities and signal indications (unless included in PTCDP)
  - How the PTCSP complies with § 236.1019(f), if applicable (attest no changes have been made to any FRA-approved main line track exceptions)
  - Any deviation in operational requirements for en route failures
    - *Make sure to provide additional PTCSP content requirement under 49 U.S.C. § 20157(j)(3)

Regulations

Other Requirements To Note:

- If a PTCSP applies to a system designed to replace an existing certified PTC system, the PTCSP will be approved provided that the PTCSP establishes with a high degree of confidence that the new system will provide a level of safety not less than the level of safety provided by the system to be replaced

- When reviewing the issue of the potential data errors (for example, errors arising from data supplied from other business systems needed to execute the braking algorithm, survey data needed for location determination, or mandatory directives issued through the computer-aided dispatching system), the PTCSP must include a careful identification of each of the risks and a discussion of each applicable mitigation

  - In an appropriate case, such as a case in which the residual risk after mitigation is substantial or the underlying method of operation will be significantly altered, the Associate Administrator may require submission of a quantitative risk assessment addressing these potential errors

Regulations

Independent Third-Party Verification & Validation:

- Is required if FRA concludes that it is necessary based on criteria set forth in 236.913, with the exception that consideration of the methodology used in the risk assessment shall apply only to the extent that a comparative risk assessment was required
- To the extent practicable, FRA will make this determination not later than review of the PTC Implementation Plan and the accompanying PTCDP or PTCSP
- The assessment may apply to the entire system or a designated portion
- The independent third-party assessment shall, at a minimum, consist of the activities and result in the production of documentation meeting the requirements of Appendix F

Regulations

Independent Third-Party Verification & Validation (Continued):

- A host railroad may submit to FRA a written request for FRA to confirm whether a particular entity would be considered an independent third party:
  - "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 PTC system supplier and vendor.
  - An entity that is owned or controlled by the supplier or vendor, that is under common ownership or control with the supplier or vendor, or that is otherwise involved in the development of the PTC system is not considered ''independent.''
- A foreign railroad regulatory entity's certification may be accepted as independently verified

Section 2:

PTC Safety Plan Conditional Approvals (Statistics)

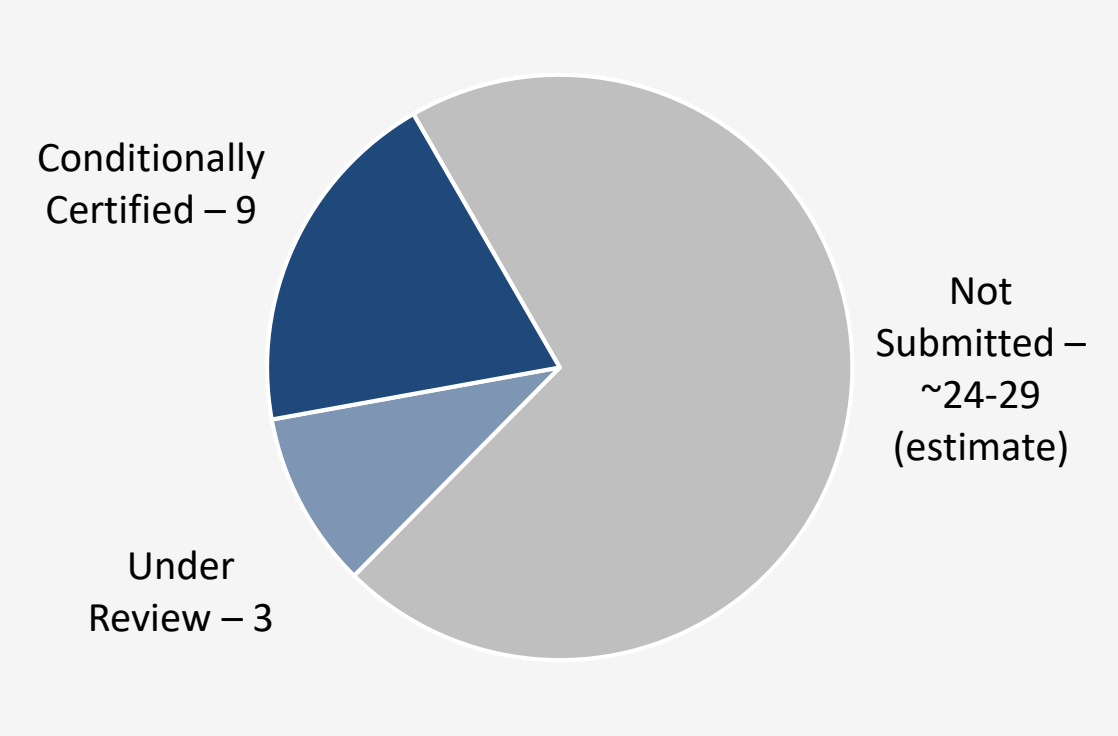
Conditionally Certified Systems

Host Railroad	PTC System	Date of Conditional Certification
Amtrak	ITCS*	December 27, 2012
BNSF Railway	I-ETMS	June 2, 2015
SEPTA	ACSES II	August 24, 2016
Metrolink	I-ETMS	September 7, 2016
CSX Transportation, Inc.	I-ETMS	September 26, 2016
Union Pacific Railroad	I-ETMS	April 26, 2017
Norfolk Southern Railway	I-ETMS	May 19, 2017
Amtrak	ACSES II	June 6, 2017
Canadian Pacific Railway	I-ETMS	June 15, 2017
Kansas City Southern Railway	I-ETMS	March 30, 2018

*ITCS received expedited certification through the 49 CFR § 236.1031 procedures, which is available only for PTC systems fully implemented prior to March 16, 2010.

PTC Safety Plan Conditional Approvals

As of August 15, 2018



Conditionally Certified:

Amtrak, BNSF, CP, CSX, KCS, NS, SCRRA, SEPTA, and UP

Under FRA Review:

CN, SDNX (NCTD), and Amtrak (I-ETMS)

PTC Safety Plan Conditional Approvals - Statistics

Key Information Regarding the 9 PTCSPs FRA Has Conditionally Approved To Date

PTC System	Conditionally Certified as	Number of Pages in Core Document	Number of Pages for All Appendices	Number of Conditions Related To Conditional Certification	Number of General Issues Requiring Resolution	Number of Specific Issues Requiring Resolution
I-ETMS	Non-Vital Overlay System	227	5113	14	26	838
I-ETMS	Non-Vital Overlay System	240	2572	13	27	727
I-ETMS	Non-Vital Overlay System	259	3943	14	28	810
I-ETMS	Non-Vital Overlay System	274	2621	13	27	596
I-ETMS	Non-Vital Overlay System	230	3096	14	26	655
I-ETMS	Non-Vital Overlay System	322	4214	14	21	212
I-ETMS	Non-Vital Overlay System	224	6127	13	25	559
ACSES II	Vital Overlay System	149	1819	14	15	198
ACSES II	Vital Overlay System	119	3785	20	12	150

PTC Safety Plan Conditional Approvals - Statistics

The 10 **core document** sections that have generated the most comments to date:

ACSES II	Average Number of Comments (ACSES II)	I-ETMS	Average Number of Comments (I-ETMS)
Railroad's PTC System Implementation	8	Railroad's PTC System Implementation	35
Safety Assessment and Application of Part 236 Appendix C	8	Safety Assessment and Application of Part 236 Appendix C	24
Risk Assessment	6	Hazard Mitigation Analysis	16
Introduction	5	Risk Assessment	15
Verification/Validation Processes	4	Verification/Validation Processes	7
Procedures, Test Equipment, O&M Manual	3	Hazard Log	7
Communication and Security Requirements	3	Potential Data Errors and Their Mitigation	6
Safety Analysis of Work Zone Incursion Protection from Human Error	3	Confirmation of FRA Type Designation for Railroad's PTC System	4
PTCPVL and Associated Errors and Malfunctions Mitigation Plan	3	General/Global	4
Configuration Management and Revision Control	3	Final Human Factors Analysis	3

PTC Safety Plan Conditional Approvals - Statistics

The 10 **appendices** that have generated the most comments to date:

ACSES II	Average Number of Comments (ACSES II)	I-ETMS	Average Number of Comments (I-ETMS)
PTC Training	23	Risk Assessment	107
System Safety Program	15	Safety Analysis	57
Manuals (except O&M)	12	Hazard Log	39
Configuration	10	Final Human Factor Analysis/Evaluation	35
Hazard Log	9	Safety Requirements	27
ACSES System Specification	7	FMEA/FFT/FTA	23
Safety Analysis	6	Operating and Support Hazard Analysis (O&SHA)	18
PTC V&V Test Results	6	Safety Assurance Concepts	16
Safety Plan	4	PTC Training	16
PTC Special Instructions	4	Preliminary Hazard Assessment (PHA)	11

Section 3:

Lessons Learned

Lessons Learned (+)

- Structure of PTCSP aligns with the content requirements of § 236.1015:
  - The PTCSP must be compliant with the requirements of § 236.1015
  - Structuring the document consistent with the regulations, including regulation references, is very helpful

- Clearly document variances to Type Approval/PTCDP:
  - The Type Approval or PTCDP is the basis of the design
  - Clearly defines differences in each railroad's PTCSP (based on railroad-specific application)
  - Enables further changes to be detailed through addendum rather than a total update to the PTCSP

- Consistent format, structure and content:
  - Some consistency in risk assessment and hazard logs
  - Some consistency in supporting design documentation
  - Some consistency in overall format and structure of the plan

Lessons Learned (-)

- 236.1015(e) calculation is a critical and mandatory element of each PTCSP:
  - Basis of the type of certification provided
  - Defines the base level of safety of the PTC system against which changes are measured
  - Has not been included in several PTCSPs
  - Is an essential element for PTC System Certification (FRA will strictly require this element to be in PTCSPs)

- The quality of a PTCSP is directly related to the duration of the review:
  - To date, FRA has identified, documented and, in many cases, corrected invalid references and statements – this model cannot be sustained
  - Poor quality documents create an immense number of conditions and comments that must be addressed (a time-consuming process)

- Railroads must own the PTCSP – it is a living, governing document:
  - It is clear many railroads have not *critically* read the full PTCSP
  - The PTCSP will form one basis for enforcement
    - The host railroad "shall implement the PTC system according to the PTCSP." 49 CFR § 236.1009(d)(3).
    - "Each railroad shall comply with all provisions in the applicable PTCDP and PTCSP for each PTC system it uses and shall operate within the scope of initial operational assumptions and predefined changes identified." 49 CFR § 236.1029(d).

Section 4:

Best Practices

Baselining, Structure & Content , and Addenda

Best Practices

Baseline

"Baseline" is an agreed description of the attributes of a product, at a point in time, which serves as a basis for defining change.

- PTC systems with varying degrees of potential for baselining:
  - I-ETMS
  - ACSES II / ASES II
  - Enhanced Automatic Train Control (E-ATC)
  - ITCS
  - Other (CBTC)?

- Would require coordination with suppliers:
  - Supplier documentation will form a key part of the baseline
  - Commitment to maintaining design configuration is essential
  - Additional coordination required when multiple suppliers are involved

- Would require configuration management and industry coordination:
  - Core set of PTC system documentation must be maintained
  - Individual railroads must document variances

Best Practices

Content & Structure

Baseline:

- Clearly specify any variances to the baseline:
  - Design, Processes, Mitigations
- Document the 'application':
  - Operating practices & procedures
  - Operating and Support Checklist Applicable to Railroads (OSCAR) and Operating & Support Hazard Analysis (O&SHA)
  - Hazard Logs & Risk Assessment
  - Railroad-specific documentation
  - PTC Product Vendor List (PTCPVL)
- Update the safety analysis:
  - To confirm level of safety is maintained or improved

No Baseline:

- Complete FRA review of entire PTCSP is required:
  - Including all product documentation
  - Complete safety analysis
  - Consider best practices

Best Practices

Addendum for Changes

- Certain changes (or additions) to a PTC system require a request to amend the PTCSP, subject to FRA approval. Some examples include:
  - Interface with a different underlying signaling or dispatch system
  - Dual operation of two different PTC systems (with different Type Approvals or PTCDPs), if the PTCSP does not already include such documentation
  - Modification of a safety-critical element of a PTC system
  - Modification of a PTC system that affects the safety-critical functionality of any other PTC system with which it interoperates

- An addendum to the PTCSP may be used to document the changes:
  - The addendum clearly documents the variances and changes
  - The fault tree, hazard analyses, risk assessment, mitigations, safety analysis and other supporting documentation must be evaluated and, if applicable, updated with respect to the change
  - Updated concept of operations and test results would be required
    - Clearly defining new interfaces and any update to the PTC system architecture
    - The railroad would also need to make any associated updates to the training plan, the security plan (i.e., the prioritized service restoration and mitigation plan), and Operations and Maintenance Manual, which must be provided to FRA upon request
  - A § 236.1035 field test request would be required for any regression testing on general rail system
  - Consider whether the change warrants a new baseline (if a baseline approach has been used)

Section 5:

PTC System Certification Going Forward

FRA PTCSP Review Process

PTC System Certification – Going Forward

To Emphasize:

- The PTCSP is the basis of any material modifications to the PTC system
- The safety analysis to calculate the level of safety improvement is the basis of the type of PTC System Certification (non-vital overlay, vital overlay, stand-alone or mixed PTC system)
- Consider lessons learned:
  - Document quality
  - Read the entire document for completeness, internal consistency and accuracy
- Consider best practices:
  - Baseline
  - Structure and content
  - Addendum approach
- PTC System Certification is required for full implementation:
  - Consider timing of submission in relation to deadlines
  - Minimum of six months for FRA review, but most submissions have taken longer
  - The FRA will be certifying approximately 25 more host railroad systems in the next 2+ years, in addition to review and approval of revised PTCSPs or addenda

PTC System Certification – Going Forward

PTCSP Review Process Going Forward:

Completeness: Confirm submitted PTCSP addresses all content requirements as required by 49 CFR § 236.1015 and 49 U.S.C. § 20157(j)(3)

Quality: Confirm accurate references, no TBAs, no incomplete sentences, no incomplete sections or unsupported statements, and a complete set of appendices

Fatal Flaws: Confirm the type of certification requested (vital overlay, non-vital overlay, stand-alone, or mixed system) is supported by the proper type of safety analysis as required by the regulations

Detailed Review: The level of detailed review will depend on the level of variance of the proposed PTC system to the Type Approval/PTCDP. There are two levels anticipated:

- If variances are documented from a baseline: The review will be more of a PTC application safety case review (does the PTC system, as implemented, operated and maintained, mitigate the design hazards and address operating hazards associated with rules & procedures)
- If there is no baseline: Both a design-based review as well as the application safety case review

Face-to-Face Meeting with Railroad: Review comments and questions, clarify any open issues to enable FRA's determination regarding approval (with conditions if needed), and, if necessary, an update to the document may be agreed upon

Decision: A decision granting or denying certification will be transmitted, with conditions if applicable, upon resolution of comments and questions

Questions and Discussion

Please see FRA's revised guidance document, dated July 24, 2018, in FRA's eLibrary at: https://www.fra.dot.gov/eLib/details/L19583#p1_z5_gD_lPO.

The guidance document addresses Operations and Maintenance Manual (OMM) requirements and the relationship between an OMM and a host railroad's PTCSP; the responsibilities of a host railroad and its tenant railroads with respect to a host railroad's PTCSP and FRA's certification of PTC systems; and interoperability testing.