Memorandum

U.S. Department of Transportation

Federal Railroad Administration

Date: APR - 1 2014

Subject: Positive Train Control Technical Bulletin PTC-14-02
Monitoring and Audit Guidelines of Positive Train Control (PTC) System Functional Testing and Track Database Verification

From: Robert C. Lauby
Associate Administrator for Railroad Safety
Chief Safety Officer

To: All Federal Railroad Administration Staff Directors, Field Employees, and Participating State Employees

The purpose of this technical bulletin is to provide the Federal Railroad Administration (FRA) Office of Railroad Safety personnel with guidance regarding the monitoring and auditing of Positive Train Control (PTC) system functional testing and track database verification.

Given the scale of PTC system implementation, direct FRA oversight of all system testing is not feasible. The alternative to FRA oversight of all testing is a combination of monitoring and auditing of railroad plans and processes. As with any oversight, there is always a degree of subjectivity that may result in a lack of uniformity. Compliance with the requirements of this technical bulletin will reduce that subjectivity and provide greater uniformity.

Even though they consist of similar tasks, auditing and monitoring are separate concepts and activities. The primary defining characteristics distinguishing auditing and monitoring are independence, objectivity, and frequency. Auditing represents evaluation activities completed by individuals, independent of the process, on a periodic basis. Monitoring represents evaluation activities completed by individuals, who may not be independent of the process, on a routine or continuous basis. Auditing should thereby provide for a more objective assessment, at least in appearance.

Auditing is a formal, systematic, retrospective, and disciplined review undertaken at points of time designed to evaluate and improve the effectiveness of processes and related controls. Detailed standards and checklists govern auditing by individuals not intimately involved in the progress of the project. An audit is an event conducted within a specified period. The outcome of an audit is a summary evaluation of attainment of quality.

Monitoring is a continuous review of the quality process based on continuous ongoing testing with the objective of collecting information for compliance with policies, procedures, and applicable laws. According to industry standards, internal controls and quality monitoring are the responsibility of business units actually carrying out the business activity. Monitoring has a formative emphasis. Feedback from the monitoring process will incorporate recommendations, and therefore contribute

directly to process procedure quality improvement Monitoring is less structured than auditing, though auditing techniques may be employed.

Whenever possible and practicable, FRA will monitor railroad initial functional testing and track database verification. In the event that FRA cannot support a railroad's monitor request, and provided the railroad has successfully passed the appropriate FRA audit, the railroad may undertake the testing without FRA monitoring. They will, however, remain subject to FRA random audits.

Functional Field Testing

FRA will review and approve all content in railroad test plans and procedures against the requirements in the attached Field Audit Checklist: Positive Train Control Systems Functional Testing Process Version 1.0. FRA will also review and approve each test procedure for compliance prior to the railroad executing the test procedure.

A railroad may not execute any test plan or procedure until it is approved by FRA. After approval, the railroad may carry out the test plan or procedure without the presence of an FRA PTC Test Monitor.

The railroad will have total responsibility for the accuracy of all aspects of the test. FRA PTC Test Monitors will randomly audit the railroad as follows:

- During a test for the railroad's compliance with the approved test plan or procedure.
- After a test has been reported as successfully completed using the "as conducted (aka redlined)" test procedure. The FRA Test Monitor will determine which of the tests reported as successfully completed by the railroad will be conducted in the presence of the FRA PTC Test Monitor. The results obtained during the test execution with the FRA Test Monitor present must match the "as conducted" test result.

A railroad not passing the audit may not conduct independent testing without an FRA PTC Test Monitor as stated below. A railroad not authorized for independent testing due to an audit failure must schedule an FRA PTC Test Monitor to be present. FRA will provide oversight support, in the order requested, as resources permit.

A railroad failing this random redlined test audit must complete, in the presence of the FRA PTC Test Monitor up to 25 percent of all tests previously reported as successfully completed using the "as conducted" (also known as redlined) test procedures. The FRA PTC Test Monitor will select the tests.

In the event another redlined test is discovered unsuccessful by the FRA Test Monitor, the railroad must complete, in the presence of the FRA PTC Test Monitor, all tests previously reported as successfully completed using, the redlined test procedure. An FRA PTC Test Monitor must also be present for up to 50 percent of all remaining tests not yet conducted.

Track Database Verification

FRA will audit a railroad's processes and procedures for track database verification using the checklist in the attached Field Audit Checklist: Positive Train Control Systems Track Database Implementation Process Version 1.0.

A railroad passing this audit may conduct independent PTC track database verification and validation anywhere on their property without the presence of an FRA PTC Test Monitor.

A railroad not passing the audit may not conduct independent verification and validation without an FRA PTC Test Monitor until they have successfully completed the audit. A railroad not authorized for independent verification and validation must schedule an FRA PTC Test Monitor to be present during any track database verification and validation. FRA will provide oversight support, in the order requested, as resources permit.

The railroad will have total responsibility for the accuracy of the database. FRA PTC Test Monitors will randomly audit the railroad for:

- The railroad's compliance with the railroad-created processes and the process initially audited by FRA.
- The accuracy of the database location of critical features that were verified and validated by the railroad.

A railroad failing this random audit:

- May not conduct independent verification and validation until all personnel involved with the database have successfully completed formal classroom and field retraining on the railroad processes and procedures to the satisfaction of the FRA PTC Test Monitor.
- Must successfully verify and validate, in the presence of the FRA PTC Test Monitor, up to 10 percent of all track previously reported as successfully verified and validated. The PTC Test Monitor will select a completed track segment for this verification and validation. In the event this verification and validation is unsuccessful, the railroad must reverify and validate 100 percent of all track previously reported as completed.

Questions regarding guidance should be directed to Dr. Mark Hartong, Senior Scientific/Technical Advisor, at (202) 493-1332 or Mark.Hartong@dot.gov.

Attachments

Version 1.0

U.S. Department of Transportation
Federal Railroad Administration

FIELD AUDIT CHECKLIST:
POSITIVE TRAIN CONTROL SYSTEMS
TRACK DATABASE IMPLEMENTATION PROCESS

Office of Railroad Safety
Washington, DC 20590

FOREWORD

This document establishes an audit plan for the review and approval of processes and procedures used by railroads in the design, implementation, test and deployment of Positive Train Control (PTC) track databases required by the Rail Safety Improvement Act of 2008 (RSIA). The guidelines in this document ensure an appropriate level of FRA oversight of track databases of PTC systems by the Office of Railroad Safety. Since it is impractical to cover all situations or conditions that may arise, the auditor must supplement them with good judgment as required.

Please forward any deficiencies, clarifications, or suggested improvements regarding the content of this document to the Signal and Train Control Division Staff Director, Federal Railroad Administration, 1200 New Jersey Avenue SE, Washington, DC 20590.

Table of Revisions

Version	Date	Notes
1.0	3/21/14	Technical bulletin routed for issuance

TABLE OF CONTENTS

Introduction

Background

Certification of PTC systems is required by 49 U.S.C. § 20157(h). This statute states "The Secretary shall not permit the installation of any positive train control 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."

A critical element of most PTC systems is the track database. The track database locates critical railroad features used by the PTC system to control train operations. These features include all integer mileposts, station signs used as designated limits, signals, switches, highway-rail grade crossings (each edge of crossing on each track), permanent speed restrictions (the begin and end limits), track detection circuits (in dark territory—the beginning and ending limits), clearance points for every switch location installed on the main and siding tracks, and any inside switches equipped with switch circuit controllers. The difference in the actual position of each of the critical features and the database indicated position of the same feature must not exceed 2.2 meters (7.2 feet).

Given the scale of PTC system implementation, direct FRA oversight of all critical features across the entire PTC network is not feasible. The alternative to verification of all data locations on each railroad is verification of the processes and procedures used by the railroads to develop and maintain the data. This verification process, when coupled with random checks of the accuracy of the data collected by the railroads, is known as risk-based oversight.

Risk-based oversight guarantees a reasonable level of oversight. Risk-based oversight is used throughout the Office of Railroad Safety to identify and resolve safety issues as well as check for regulatory compliance, with the most notable being the National Inspection Plan.

Scope and Purpose

The audit plan proposed in this document accomplishes two specific objectives. The first is to ensure individual railroads have implemented processes and procedures that, if followed, will result in the safe and effective creation and maintenance of PTC track databases with less direct FRA oversight. Railroads that continue to satisfy the best practices of this checklist will only require random FRA audits for compliance. However, if necessary, FRA will increase the frequency and scope of audits should circumstances warrant it.

The second objective is to provide FRA personnel with a better understanding of the railroads' PTC-related processes to facilitate FRA review and understanding of the role of the safety case presented in the PTC Safety Plan (PTCSP) submitted by each railroad.

.

As with any audit, there is always a degree of subjectivity between different auditors. This may result in a lack of uniformity in the audit of results. Compliance with the requirements

of this document should reduce that subjectivity and provide greater uniformity of the audits. Each audit will vary slightly depending on the individual railroad property and their approach to system safety.

This document is not a substitute for good judgment, experience, and common sense.

As is the case with other regulatory requirements, responsibility for compliance is with the railroads. The railroad retains ultimate responsibility, not only for their actions, but also for the actions of their contractors and subcontractors.

Minimum Track Database Creation and Maintenance Requirements

These requirements outline the minimum policies and procedures to be implemented by railroads to ensure the necessary accuracy of the track database in support of their PTC operations. Railroads whose database data collection and maintenance processes and procedures satisfy these conditions will be subject to random FRA audits for compliance. While the requirements describe the various functionalities that FRA is expecting, each railroad is able to develop processes, plans, and procedures best suited to their own business model, with the stipulation that the processes and procedures clearly detail all of the actions required by all of the affected employees.

The requirements for each functional attribute that must be addressed by the railroad are as follows:

- Definition of requirement (Definition).
- Goal of requirement, which is the desired outcome of adhering to the best practice for the problem (Goal).
- Best Practice to satisfy the goals FRA expects to be implemented as part of the railroad's database management plan (Best Practice).

Governance Management Requirements

1. Definition
   Governance management is a business process that addresses the management structure for control of the database process and the coordination of the activities of the associated plans and processes.

2. Goal
   Governance management accomplishes one or both of following things. First, it aggravates the individual processes and procedures associated with creation and maintenance of the track database. Second, it defines roles and responsibilities of the railroad organizations and individuals that participate in the process.

3. Best Practice
   a. Railroad Stakeholder Driven
      To reflect the business needs of participants in the enterprise, the governance process is driven from a railroad stakeholder perspective. This may take many

structural forms, from a democratically structured board of directors to advisory councils. Minimally, the interests of all parties in the railroad associated with the design, implementation, population, and maintenance of the database must be formally heard and acknowledged.

b. Review and Oversight
Review of the accuracy of the database governance processes and procedures and applicability should on an annual basis.

c. Accountability
To be meaningful, success of the processes and procedures associated with governance management should be measured in either quantitative (performance metrics) or nonquantitative terms (qualitative outcomes). The criteria for success should be determined prior to the period of performance. Success criteria should be developed with the railroads' stakeholders and should be continuously monitored so that corrective actions may be taken to tactics, resources, and, if necessary, strategies. Status of the success criteria should be published and accessible to all stakeholders. If possible, rewards or at least acknowledgement for exceeding performance should be offered.

Organizational Communication Requirements

1. Definition
Organizational communications are the processes and procedures necessary to support database creation, implementation, and maintenance. Because the track database is central to the safe operation of most PTC systems, it is important that communication is formalized, timely, and persistent among users, maintainers, developers, and system administrators within the railroad. What are described here are appropriate communicative responses to common events. The events identified concern data, applications, hardware, software, and personnel. The proposed responses include communication methods that are tailored to the appropriate audience and urgency of the message.

2. Goal
The goal of communication is to provide sufficient information to all railroad track database users, maintainers, developers, and system administrators about events that may impact data, systems, applications, operations, and staff. There may be substantial support or evidence of partial forms of some or all of these components activities.

3. Best Practice
Written plans and procedures for the following activities must be in place for:
   a. Announcement of events impacting all stakeholders of the database.
   b. Creation of new critical attributes in the database.
   c. Changes in existing critical attributes n the database.
   d. Deletion of existing critical features in the database.
   e. Discovery of data errors associated with critical attributes.
   f. Correction of data errors associated with critical attributes.

g. Railroad governance changes impacting any aspect of the database design, population, maintenance, and retirement.
h. Planned production database server outage.
i. Unplanned production database server outages.
j. Identification of staff changes associated with database governance.
k. Addition of new software applications associated with the design, implementation, and maintenance of the database.
l. Modification of the software application associated with the design, implementation, and maintenance of the database.
m. Changes to the supporting database communications networks.
n. Database server replacement/upgrades.
o. Database server retirement.
p. Database software upgrades/reconfiguration.

Minimum Data Standards Requirements

1. Definition
   Data standards provide a definition or format that has been approved by an internal review committee, a recognized standards organization, or is accepted as a *de facto* standard by an industry. Data standards could also be referred to as protocols, specifications, application protocols, and technical standards. Clearly established data standards facilitate the development, sharing, and use of spatial data.

2. Goal
   Data has to meet minimum standards for quality, accuracy, and consistency prior to being accepted into the database repository.

3. Best Practices
   a. All production data in the production track database is verified for projection, precision, and topology prior to insertion into the database. The plans and procedures associated with this are documented.
   b. Data already existing in the database goes through a certification process to determine if it meets current data standards. If not, appropriate remediation will be implemented with the notification provided. The plans and procedures associated with this are documented.
   c. Consistent measurements to determine the quality of data are implemented to continuously monitor and analyze data improvements over time. The plans and procedures associated with this are documented.
   d. Accuracy of positional data must be within 2.2 meters (7.2 feet) or better horizontally.
   .

Minimum Data Quality Assurance Requirements

1. Definition
   Quality assurance concerns the enforcement of integrity and correctness of data posted in a database.

2. Goal
   All production data in a database must meet minimum collection and publication standards.

3. Best Practices
   a. Track Database Data Collection
      Data collection and maintenance tasks include strict data integrity checks at the point of data entry. Data quality is protected from routine typographical errors, inaccurate values, and inconsistent entry practices through the use of pull-down selection menus of valid values, notification of invalid or duplicate entries, confirmation to commit prompts, and other automated data entry aids. The plans and procedures associated with this are documented.
   b. Track Databases Publication
      Data submitted for use in the track database will be tested for data standards compliance prior to insertion. Any data failing to meet standards requires that the designated manger be notified, with clear and concise descriptions of the reason for rejection along with possible solutions for alleviating the problems cited. The plans and procedures associated with this are documented.

Track Data Access Requirements

1. Definition
   Railroad employees require access to the database information. The amount and type of information may vary depending on the organizational role. This allows for the possibility that not all users need the same access for all data.

2. Goal
   Provide appropriate user definition and access to data.

3. Best Practice
   a. Railroad maintains separate access control for production and nonproduction track data. The plans and procedures associated with this are documented.
   b. Each railroad user only has access to the data required by their role. The plans and procedures associated with this are documented.
   c. Database access is cataloged and indexed to meet railroad-specified security requirements. The plans and procedures associated with this are documented.
   d. There is no change allowed to production data. Changes to production data must first be made on the nonproduction server and then transferred to the production server. The plans and procedures associated with this are documented.
   e. Changes to the production data or database access by a single individual must be independently checked. The plans and procedures associated with this are documented.

Track Database Data Currency Requirements

1. Definition
   Data currency standards concern the timeliness of the delivery and review of all data provided to the database.

2. Goal
   Data currency standards ensure data provided to database are the most up-to-date data and that historical data is clearly identified, removed, or archived.

3. Best Practice
   The person designated in writing as the data custodian assumes the following responsibilities with regard to posting data:
   a. Data that is obsolete or inaccurate over time is be updated at an interval that is appropriate as established by the governance organization. The plans and procedures associated with this are documented.
   b. Notification of data update completion is made to database users. The plans and procedures associated with this are documented.
   c. Changes to track data other than that specified and approved by the governance structure are prohibited. When an update occurs in one data set that is the source for derivative data sets (e.g., any summarized data that is obtained from a more detailed source), a process is implemented and documented that coordinates the update of all dependent data sets. The plans and procedures associated with this are documented.
   d. Data that does not become invalid over time and that does not require changes must be identified, annotated, and an appropriate explanation about the lack of updates recorded.

Track Database Data Publication Requirements

1. Definition
   Publishing the most current data prevents confusion among users.

2. Goal
   Data published should be the most current available.

3. Best Practices
   a. Corrected or changed data is refreshed in the database on a regular schedule agreed to by the governance management. The plans and procedures associated with this are documented.
   b. All data published has dates associated with the data so users know what currency limitations may apply. The plans and procedures associated with this are documented.
   c. Prior to publishing data, the publisher notifies the custodian or owner of the data that the data would be accessible. The plans and procedures associated with this are documented.

Track Database Data Redundancy Requirements

1. Definition
   Data redundancy standards address instances where there appears to be multiple occurrences of the same information in separate data sets.

2. Goal
   Data redundancy standards ensure that duplication of information in different data sets occurs only when data sets have clearly divergent and defined differences in purpose.

3. Best Practice
   The data custodian assumes the following responsibilities in regards to redundant data:
   a. If another data set exists with similar information, the data custodian of the newly created data contacts the existing data set's custodian to determine whether the currently posted data set can be modified, updated, or merged with the new data set to meet the identified needs. The plans and procedures associated with this are documented.
   b. If data sets covering similar information must co-exist, the data custodians of those data sets must:
      i. Coordinate where possible any data updates for portions of the data set that are similar between the data sets to avoid duplication of effort.
      ii. Clearly define in the metadata, with references to the similar data sets available, which data set is appropriate for which conditions and uses.

   The plans and procedures associated with this are documented.

Track Database Data Replication Requirements

1. Definition
   Production data is copied or replicated from the primary production database to a secondary storage location for purposes of security, safety, of other business need.

2. Goal
   To maintain data currency and keep data sets maintained and synchronized on multiple servers.

3. Best practice
   a. Replicated copies of data are not be modified on the secondary site.
   b. New or modified data on the secondary server is refreshed from the primary server on a regular, agreed to schedule that is documented using appropriate plans and procedure.
   c. Currency of replicated data is with the responsibility of the administrator of the secondary site. The plans and procedures associated with this duty are documented.

d. If the data changes format during or in support of replication (i.e. from coverage to shape file or some other format), the data quality is checked to prevent corruption. The plans and procedures associated with this are documented.
e. The primary database administrator is to be notified when a data set is replicated on any secondary server site. Notification will include a contact name, and full documentation of the replication process frequency and timing. The plans and procedures associated with this are documented.

Data Creation and Work Procedures Requirements

1. Definition
   Documented work procedures, plans, and processes define who or what work group is responsible for creating and maintaining data. Data creation and work procedures aid staff training and assure consistent practices and workflow.

2. Goal
   All recurring and nonrecurring work procedures are to be well documented.

3. Best Practice
   a. Work processes (plans and procedures), both for individuals and for groups, are evaluated for recurring, predictable procedures. When these plans and procedures are identified, procedural documentation will be prepared and kept in a place that is readily accessible for all work group employees.
   b. Procedural documentation is a step-by-step description of the tasks necessary to perform a given work procedure, written in as much detail as is useful for ongoing maintenance of the database.
   c. This documentation is maintained current, cataloged, and accessible.

Database Data Migration Requirements

1. Definition
   Database data migration is the conversion of data in one format to data in a different format.

2. Goal
   Any conversion or migration of production data that requires a formal migration plan. The purpose of a data conversion or migration plan is to lessen the potential negative effects and increase the potential positive effects that data conversion or migration could have on existing projects and processes.

3. Best Practice
   a. When data migration or conversion is proposed that will affect data commonly used (as opposed to data stored and/or used by a single individual), a data migration or conversion plan and procedure is created through a collaborative process with all potentially affected parties.

b. The data conversion plan and procedure evaluates the current data format and structure, the proposed data format and structure, a description of the proposed process of migrating the data from one to the other, and any impacts on applications and operations that the conversion will have, along with proposed remedies for the identified impacts.
c. The data migration plans and procedures evaluate the current data format and structure, the proposed data format and structure, the proposed migration process, and any impacts on applications and operations that the conversion plan and procedure will have, along with proposed remedies for the identified impacts.
d. The actual data migration or conversion process is documented.

Data Custodian Requirements

1. Definition
   Data custodians are required to manage their assigned data attributes, including:
   a. Making sure that processes required to post attribute values to the track database are correctly followed.
   b. Documenting the data attributes to ensure proper interpretation and to safeguard against misuse or accidental loss.
   c. Ensuring the data is available.

2. Goal
   The goal is to have a clear point of contact and responsibility for all elements of the database as well as the associated processes and procedures.

3. Best Practice
   a. The person creating the process and procedures used are identified. The plans and procedures associated with this are documented.
   b. Shared databases are assigned to a single custodian. The plans and procedures associated with this are documented.
   c. Primary and secondary points of contact for the databases are assigned and documented. The process for changing, replacing, or reassigning the staff members serving as a custodian is documented.
   d. Persons needing more information regarding the database attributes have a process or procedure to follow to contact the data custodians assigned to those attributes.

Metadata Content Requirements

1. Definition
   Metadata or “data about data” describes the content, quality, condition, and other characteristics of the data. It captures information about the data so both users and maintainers have a clear understanding of issues relative to data maintenance, collection, and use.

2. Goal
   Current, descriptive metadata for all track database data is available, and the process and procedures for accessing the information are documented.

3. Best Practice
   The Federal Geographic Data Committee approved the Content Standard for Digital Geospatial Metadata or a documented equivalent defined for the data. The following minimum elements of information about the data are required:
   a. Data element identification name.
   b. Data originator (organizational element and data steward contact person), publication date, presentation form.
   c. Data description: abstract, purpose, access constraints, native data set format.
   d. Data quality information: attribute accuracy report, completeness report.
   e. Effective time period: currency reference and date.
   f. Status of data: stage of progress in collection, update frequency.
   g. Spatial domain: bounding coordinates (North, South, East, West).
   h. Search keywords: theme.
   i. Custodian point of contact: organization and contact person (name, organization, phone number, email address).
   j. Spatial reference: horizontal coordinate system information.
   k. Entity and attribute: for each entity type, label and define (optional). For each attribute, label and define.
   l. Metadata reference: metadata date, metadata standard name, metadata contact person (name, organization, phone number, email address).
   m. Distribution information: distributor contact person (name, organization, phone number, email address), distribution liability

   The plans and procedures associated with this are documented.

Metadata Development and Maintenance Tools Requirements

1. Definition
   These are the tools used to create and maintain the metadata.

2. Goal
   Tools for the creation and maintenance of the metadata are documented and used.

3. Best Practice
   a. Railroad uses a metadata tool that is flexible, supports manual edits or corrections to automatically generated content, and supports different versions of metadata (e.g., production and publication metadata).
   b. Where possible, railroad populates and maintains metadata using available functionality imbedded in current database software.
   c. Railroad has processes and procedures to manually correct or modify metadata files as needed to make the content more accurate and useable for the specific end user audience.

Audit Checklist

Audit checklists support regulatory oversight of performance-based regulations. They focus the auditors on critical process attributes that the railroads' processes and procedures must address. Audit checklists also provide the regulator a mechanism for identifying critical performance concerns of the regulated entity, and provide a baseline for the regulated entity to develop appropriate processes and procedures. The checklist in Appendix A should be used to facilitate and provide guidance for the creation, review, and audit of the railroads' track database creation and maintenance processes. The checklist has been created primarily considering general situations. Particular projects may have other unique project requirements, and the checklist in Appendix A should be tailored to make it more effective and efficient. Keep in mind that the main idea is that there should be a systematic review of requirements based on a checklist that makes sense for your project

Virtually all elements associated with the checklist in Appendix A require written plans, processes, procedures, and polices There are differences that must be considered when evaluating compliance with the audit requirements. Policy is a set of ideas or a plan of what to do in particular situations that has been officially agreed upon. A plan is a detailed proposal for doing or achieving something. A plan implements policy. It identifies the various processes required. A process defines "what" needs to be done, and the various roles that are involved. It outlines the roles and responsibilities of the people assigned to do the work, the appropriate tools and equipment to support individuals in doing their jobs, the procedures and methods defining "how" to do the tasks, and relationships between the tasks. A procedure defines how to do a task, and is usually associated with a subset of the roles involved.

This checklist should not be used in a simple "yes/no" manner. The idea is to consider what might be possible, and then determine what is feasible. The checklist should be reviewed periodically. Users of this checklist may find it helpful to rephrase questions in order to prompt maximum creativity; for example "how might it be possible to...?"

Appendix A: Audit Checklist

Audit Element	Audit Attribute	Y	N	Comments
1.	The railroad has identified senior management staff (mechanical, signal, operating, track, and IT personnel) ultimately accountable for database accuracy in writing.			
2.	The railroad has specified in writing, the responsibilities of all personnel (management, mechanical, signal, operating, track, and IT personnel) who interact with the database.			
3.	The railroad has a current organization chart that shows the relationship between personnel (mechanical, signal, operating, track, and IT personnel) involved with database development and maintenance.			
4.	The railroad has specified in writing all contractor personnel who have access to the database.			
5.	The railroad has specified in writing the limits of contractor access to the database.			
6.	The railroad has established written access control polices for railroad personnel (mechanical, signal, operating, track, and IT personnel).			
7.	The railroad has established written access control policies for contractor personnel.			
8.	The railroad has written plans and procedures for announcing changes in staff (mechanical, management, operating, signal, IT) responsible for management of database data.			
9.	The railroad has established written database recovery plans and procedures for continuity of operations (COOP).			

10.	The railroad has established UPTIME, MTTF, and MTTR performance goals for the database and supporting equipment.			
11.	The railroad has written plans and procedures for regularly evaluating the degree of obtainment for UPTIME, MTTF, and MTTR performance goals.			
12.	The railroad has written plans and procedures for announcing planned database outages to all end users.			
13.	The railroad has written plans and procedures for announcing unplanned database outages to all users.			
14.	The railroad has established written plans and procedures for identification of any database errors.			
15.	The railroad has established written plans and procedures for adjudication of any database errors.			
16.	The railroad has established written plans and procedures for cancellation of user database access.			
17.	The railroad has sufficient software licenses for all software used.			
18.	The railroad has written plans and procedures to ensure the software versions used are correct.			
19.	The railroad has written plans and procedures for making changes to the database software.			
20.	The railroad has written plans and procedures for deletion of database software.			
21.	The railroad has written plans and procedures for contacting all users of the database.			
22.	The railroad has written plans and procedures for the designation of critical features in the database.			
23.	The railroad has written procedures for addition of new critical features to the database.			

24.	The railroad has written plans and procedures for changes in the critical features in the database.			
25.	The railroad has written plans and procedures for deletion of existing critical features in the database.			
26.	The railroad has written plans and procedures for field forces upon discovery and reporting of errors in critical features or location in the database.			
27.	The railroad has written plans and procedures for office forces upon discovery and reporting of critical feature errors in the database.			
28.	The railroad has written plans and procedures for field personnel correction of errors associated with critical features in the database.			
29.	The railroad has written plans and procedures for office personnel correction of errors associated with critical features in the database.			
30.	The railroad has written plans and procedures for creation of the data that will be placed in the database.			
31.	The railroad has written plans and procedures for verification and validation of data that will be placed in the database.			
32.	The railroad has written plans and procedures for correction of data errors in the database.			
33.	The railroad has written plans and procedures for the deletion of data in the database.			
34.	The railroad has written plans and procedures for establishing new communications paths.			
35.	The railroad has written plans and procedures for pushing database changes to distributed computers and servers.			
36.	The railroad has written plans and procedures for backing up the database.			

37.	The railroad has written plans and procedures for the recovery of the database.			
38.	The railroad has written plans and procedures for upgrading the database and server.			
39.	The railroad has written plans and procedures for retirement of a database.			
40.	The railroad has written plans and procedures for field verification and validation of database data prior to insertion into the database.			
41.	The railroad has written plans and procedures for office verification and validation of database data prior to insertion into the database.			
42.	All positional data is accurate to within 2.2 meters (7.2 feet) horizontally.			
43.	The railroad has written plans and procedures for collection of field data.			
44.	The railroad has written plans and procedures for periodic reverification and revalidation of the accuracy of the data.			
45.	The railroad has written plans and procedures for sharing data externally and internally.			
46.	The railroad has written plans and procedures for the segregation of production (verified and validated data) and data that has not been verified or validated.			
47.	The railroad has written configuration management plans and procedures for the track database and data.			
48.	The railroad has written plans and procedures for notification of tenant railroads of track database-related issues.			

49.	All written plans and procedures associated with database creation, and maintenance are under configuration management.			
50.	All written plans and procedures are accessible to the appropriate workforce.			
51.	There are written plans and procedures for duplication and distributions of a duplicated database.			
52.	The railroad has written plans and procedures to verify there is a single master database.			
53.	Data conversion software is under configuration control.			
54.	Data conversion software has proof of sufficient testing for demonstration of correctness (input, output, boundary conditions).			
55.	Inputs and outputs of data conversion software are defined along with boundary conditions for data.			
56.	Data conversion and migration plans, procedures, and processes have been approved by the governance organization.			
57.	A primary and secondary database has been designated.			
58.	There is a detailed published data format standard.			
59.	There are documented integrity checks for all data used to evaluate data prior to submission to the database.			
60.	The railroad has written plans and procedures to verify changes cannot be made directly to production data on production servers.			
61.	Data is validated and verified independently prior to submission to the production server. This is documented.			

62.	There are written policies, plans, and procedures for periodic data updates.			
63.	There is a documented policy that precludes changes to track database data without approval of the governance entities.			
64.	Track database data that does not change over time is documented and the reason why it is unchanged is explained.			
65.	There are procedures and processes for the periodic refresh of database track data.			
66.	There are written plans and procedures for notification of a completed data upload.			
67.	Duplicate data is clearly identified, along with the reason for duplication.			
68.	The conditions under which each of the duplicated data is allowed to be used is defined in writing.			
69.	There are written plans and procedures to address handling of discovery, maintenance, and upkeep of duplicate data for currency and accuracy.			
70.	There are written policies that preclude modification of replicated data on an alternate (COOP) server site.			
71.	There are written processes and procedures for the update of replicated data from the primary to the secondary (COOP) server.			
72.	There are written processes and procedures for validation of data transfer from the primary to the secondary site.			
73.	There are written processes and procedures to notify the primary database administrator when data is transferred to the secondary site.			
74.	All nonrecurring and recurring work procedures are documented.			

75.	All recurring work procedures reflect completion of a task analysis.			
76.	There is a documented periodic training plan for all employees whose work results in a direct or indirect interaction with the track database.			
77.	Successful completion of training is documented.			
78.	Data custodians are designated in writing.			
79.	Data custodians have all completed documented periodic training appropriate to their roles.			
80.	All databases have a single primary and secondary point of contact.			
81.	There are documented processes and procedures for reassignment and change in primary or secondary custodians.			
82.	There are written polices, plans, procedures, and processes for obtaining information regarding any specific database and its contents.			
83.	All metadata regarding the data has been documented.			
84.	All metadata for data follows the Federal Geographic Data Committee approved Content Standard for Digital Geospatial Metadata or documented equivalent.			
85.	Any metadata development tools are documented.			

Version 1.0

U.S. Department of Transportation
Federal Railroad Administration

FIELD AUDIT CHECKLIST: POSITIVE TRAIN CONTROL SYSTEMS FUNCTIONAL TESTING PROCESS

Office of Railroad Safety
Washington, DC 20590

FOREWORD

This document defines a set of minimum actions for the evaluation of a railroad's functional testing of its Positive Train Control (PTC) system. The Office of Railroad Safety guidelines in this document ensure an appropriate level of verification and validation of functional testing in support of PTC System Certification required by the Rail Safety Improvement Act of 2008 (RSIA). Since it is impractical to cover all situations or conditions that may arise, the auditor must supplement them with good judgment as required.

Please forward any deficiencies, clarifications, or suggested improvements regarding the content of this document to the Signal and Train Control Division Staff Director, Federal Railroad Administration, 1200 New Jersey Avenue SE, Washington, DC 20590.

Table of Revisions

Version	Date	Notes
1.0	3/21/14	Technical bulletin routed for issuance

TABLE OF CONTENTS

Introduction

Background

Certification of PTC systems is required by 49 U.S.C. § 20157(h). This statute states "The Secretary shall not permit the installation of any positive train control 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."

A critical element of PTC System Certification is that the Federal Railroad Administration (FRA) can reasonably determine if a railroad's engineering and test efforts demonstrate that the PTC system implements the required core functions:

- Reliably and functionally prevent train-to-train collisions.
- Reliably and functionally prevent overspeed derailments.
- Reliably and functionally prevent incursions into established work zone limits without first receiving appropriate authority and verification from the dispatcher or roadway worker in charge, as applicable.
- Reliably and functionally prevent the movement of a train through a mainline switch in the improper position.
- All while trains are operating seamlessly across and between different railroads.

Given the scale of PTC system implementation, direct FRA oversight of all system testing is not feasible. The alternative to FRA oversight of all functional testing is verification of the processes and procedures used by the railroads to plan and conduct the required testing. This verification process, when coupled with random checks of the railroad's compliance with the railroad's test plans and procedures, is known as risk-based oversight.

With risk-based oversight, there is no guarantee that all data collected is sufficiently accurate, complete, or collected and maintained in accordance with the railroad's processes and procedures. Instead, it guarantees a level of oversight that would be expected by a "reasonable man." A reasonable man is a hypothetical person who exercises average care, skill, and judgment in conduct and who serves as a comparative standard for determining liability.

The use of risk-based oversight is not without precedence in FRA. Risk-based oversight is used throughout the Office of Railroad Safety to identify and resolve safety issues as well as check for regulatory compliance, with the most notable being the National Inspection Plan.

Scope and Purpose

A fundamental limitation of any test program is that it cannot assure that upon completion there are no latent or hidden faults that prevent the core functions from operating correctly. At best, a test program can (1) only detect the presence of faults and (2) provide reasonable assurance that the probability of occurrence of these faults is reduced to acceptable levels.

The audit plan proposed in this document accomplishes two specific objectives. The first is to ensure individual railroads have implemented processes and procedures that, if followed, will result in the safe and effective testing of the railroad's functional behaviors with less direct FRA oversight. Railroads who continue to satisfy the best practices of this checklist will only require random audits by FRA for compliance. However, if necessary, FRA will increase the frequency and scope of audits if circumstances warrant.

The second objective is to provide FRA personnel with a better understanding of the railroad's PTC-related processes to facilitate FRA review and understanding of the role of the safety case presented in the PTC Safety Plan (PTCSP) submitted by each railroad.

As with any audit, there is always a degree of subjectivity that may result in a lack of uniformity. Compliance with the requirements of this document should reduce that subjectivity and provide greater uniformity of the audits. Each audit will vary slightly, depending on the individual railroad property, the PTC system they chose to implement, and their approach to system safety.

This document is not a substitute for good judgment, experience, and common sense.

As is the case with other regulatory requirements, responsibility for compliance is with the railroads. The railroad retains ultimate responsibility not only for their actions, but also for the actions of their contractors and subcontractors.

Test Plan and Procedures

Test plans and procedures are two very different, but related tasks. A test plan documents the strategy that will be used to verify and ensure that a product or system meets its design specifications and other requirements. A test procedure is a formal specification of test cases to be applied to one or more target functions modules. Test procedures are executable and are complete, self-contained, self-validating, and execute automatically. Test procedures are a deliverable product of the software development process and are used for both initial checkout and subsequent regression testing of program modifications.

Requirements should include derived safety requirements, and any additional mitigation requirements, based on initial and subsequent hazard analysis. Since the safety analysis should continue throughout the development and procurement processes, requirements can and should be expected throughout the development and procurement process. The need to provide correct data over interfaces will usually be a source of derived safety requirements for complex electronic systems (e.g., for message integrity protocols). Derived safety requirements may include logical invariant relationships, functions and definitions (including transitions and actions), sequencing, and timing.

Since it is not realistic to assume that a complex electronic element can be error free, the quantitative safety integrity requirements should specify the tolerable failure rate. It is possible for the violation of some derived safety requirements to directly contribute to an accident, especially if the derived safety requirement is a single point of failure. The safety

integrity requirements should be progressively refined to a level of detail that is sufficient to specify and perform verification and validation of the software and hardware components.

All railroad test plans have specific elements that must be addressed. There are a number of different formats that may be used to present the information. IEEE 829, also known as the "Standard for Software and System Test Documentation," is perhaps the most widely used. While it is not required that a railroad use the IEEE 829 format for their test plans, it is highly encouraged. A railroad may elect to use any format they desire, with the caveat that they must be able to show where the information that is specified in IEEE 829 is located. If it cannot be clearly determined what parts of a submitted document address the information requirements outlined in IEEE 829, then it will be assumed the submitted document does not address the information.

Minimal Test Plan Contents

IEEE 829 is an IEEE standard that specifies the form of a set of documents for use in eight defined stages of software testing, each stage potentially producing its own separate type of document. The standard specifies the format of these documents, but does not stipulate whether they all must be produced, nor does it include any criteria regarding adequate content for these documents. The content of the documentation will vary depending upon the complexity of the system and the criticality of the functions being tested.

The test plan defines the test environments, including site locations, hardware and software components, test equipment, and personnel needed for the tests. It identifies the type (class or category) of tests to be performed, test objectives, test level, verification methods, special requirements, recording, reduction, and analysis needed for each of the identified types of tests to be performed. It also provides the test schedules for each test. Most importantly it provides traceability from each identified test to the system requirements and vice versa. The following information outlines the minimal test plan informational requirements:

1. Introduction
   This is an executive summary of the plan (purpose, scope, etc.).

2. References
   These are the:
   A. System requirements documents with the requirements that drive the system-level tests.
   B. Architectural design documents with the architecture that drives the subsystem and integration testing.
   C. Other documents such as detailed design data, standards, sample plans, etc. that are test drivers.

3. Test Items
   These are the:
   A. Version of product being testing at each stage of the testing.

   B. Relationship of the system requirements and architectural elements to the test plan and test cases.
   C. Limitations of the product under test (restrictions, assumptions, caveats, etc.).
   D. Other product-level restraints on testing.

4. Risks
   These are the:
   A. Specific risks that may affect testing or the test outcome, including safety and performance items and constraints.
   B. Risk mitigation plan for these risks.

5. Functions to be Tested
   This is a list of specific functions that will be tested.

6. Functions not to be Tested
   This is a:
   A. List of those functions that cannot or will not be tested.
   B. The rationale for not testing each item (for example: not in current release, insufficient test capability, low risk function that is hard to test, not a user-visible feature, etc.).

7. Approach or Strategy
   This is the:
   A. Overall test strategy (what, why, and how of the test plan).
   B. Number of hardware and software configurations tested or not tested.
   C. Plan to deal with defects identified (regression testing).
   D. Metrics identified for overall success (number of bugs found/corrected/open, number of critical features passed, etc.).
   E. Special requirement for testing.

8. Item Pass/Fail Criteria
   This is the specific pass/fail criteria for each feature to be tested (number and severity of defects, any specific tests that indicate system failure, etc.).

9. Test Deliverables
   This is a list of what is to be delivered by this test plan (plan document, test procedures, error logs, etc.).

10. Test Schedule for Test Procedure Execution

11. Plan Approvals

Minimal Test Procedure Contents

Just as test plans define the test environments and tests that will be conducted, the test procedures provide the detailed instructions of how the tester will physically run the test, the

physical setup required, and the procedure steps that need to be followed. It also provides traceability from each identified test to the system requirements and vice versa. The following outlines the minimal test procedure informational requirements.

1. Identification
   This is a unique identifier of the test, the system, and the software that the procedure applies, including, as applicable, titles, abbreviations, version numbers, and release numbers.

2. Referenced Documents
   This lists the number, title, revision, and date of all documents referenced in the procedure.

3. Test Preparations
   A. Hardware preparation
      This describes the procedures necessary to prepare the hardware for the test. The following are provided, as applicable:
      i. The specific hardware to be used, identified by name, and, if applicable, number.
      ii. Any switch settings and cabling necessary to connect the hardware.
      iii. One or more diagrams to show hardware, interconnecting control, and data paths.
      iv. Step-by-step instructions for placing the hardware in a state of readiness.

   B. Software preparation
      This describes the procedures necessary to prepare the items under test and any related software, including data, for the test. The following are provided, as applicable:
      i. The specific software to be used in the test.
      ii. The storage medium of the items under test (e.g., magnetic tape, diskette).
      iii. The storage medium of any related software (e.g., simulators, test drivers, databases).
      iv. Instructions for loading the software, including required sequence.
      v. Instructions for software initialization.

   C. Other pretest preparations
      This describes any other pre-test personnel actions, preparations, or procedures necessary to perform the test.

   D. Assumptions
      Any assumptions made and constraints or limitations imposed in the description of the test case due to system or test conditions, such as limitations on timing, interfaces, equipment, personnel, and database or data files. If waivers or exceptions to specified limits and parameters are used, they must be identified and their effects and impacts upon the test procedure explained.

4. Requirements Addressed
   This identifies the application or system requirements addressed by the test procedure. This includes traceability from each test procedure to the application requirements it addresses. If a test procedure addresses multiple requirements, traceability from each set of test procedure steps to the requirements is addressed.

5. Other Prerequisite Conditions
   This identifies any additional prerequisite conditions that must be established prior to performing the test.

6. Test Inputs
   This describes the test inputs necessary for the test procedure. This includes:
   A. Name, purpose, and description (e.g., range of values, accuracy) of each test input.
   B. Source of the test input and the method to be used for selecting the test input.
   C. Whether the test input is real or simulated.
   D. Time or event sequence of test input.
   E. The manner in which the input data will be controlled.

7. Expected Test Results
   This paragraph describes all expected test results for the test case. Both intermediate and final test results shall be provided, as applicable.

8. Criteria for Evaluating Results
   This identifies the criteria to be used for evaluating the intermediate and final results of the test case.

9. Test Procedure Steps
   This defines the details of the test procedure. The test procedure is defined as a series of individually numbered steps listed sequentially in the order in which the steps are to be performed. The appropriate level of detail in each test procedure depends on the test being performed. The appropriate level of detail is the level at which it is useful to specify expected results and compare them to actual results. The following must be provided for each test procedure, as applicable:
   A. Expected result and evaluation criteria for each step.
   B. If the test case addresses multiple requirements, identification of which test procedure steps address which requirements.
   C. Actions to follow in the event of a program failure or indicated error.
   D. Procedures to be used to reduce and analyze test results.
   E. Evaluate output as a basis for continuation of test sequence.
   F. Evaluate test output against required output.

10. Notes
    Any general information that aids in understanding of the procedure (e.g., background information, glossary, rationale, acronyms, abbreviations, and their meanings, terms and definitions, etc.).

11. Procedure Approvals

Classes of Evidence

In order to evaluate if the test plan, procedures, and results provides the required evidence that a functional behavior has been validated, it is necessary to have a basic understanding of the various types of evidence that may be provided by a railroad. There are a number of different types of evidence that may be presented, some or all may be appropriate, and the use of one class of evidence as opposed to another is not grounds for automatic rejection of the argument that a functionality has been satisfactorily provided. Provided the class of evidence and the associated technical argument are valid, any approach may be acceptable. Because of this, the auditor must not only understand what types of evidence may be provided, but also apply good technical judgment when evaluating the evidence.

The body of evidence provided by the railroad is likely to be extensive. In general, this evidence may be broken into three classes:

1. Direct evidence
2. Process evidence
3. Counter evidence

Direct evidence is associated with the performance of the system in an operational or simulated environment. Direct evidence may also relate to the requirements, role, or mitigation associated with the use of the complex electronic element in its system context. Process evidence is evidence about the processes used for the creation of the system for risk assessment, procurement, development, verification, validation (including demonstration), or operation of the complex electronic element. Such process evidence serves to increase confidence in the direct evidence. Counter evidence is the demonstration that the presence of a fault or failure does not adversely affect the safety case.

The quality and quantity of evidence provided should be proportionate to the level of safety required. The evidence should be selected so that it supports claims for the safety of the system. Evidence should be traceable by means of arguments to claims that it supports the system requirements and the derived requirements. The claims should typically address the correctness and sufficiency of the safety requirements (including safety integrity requirements) and the satisfaction of the safety requirements. The claims must also demonstrate how failure rates of components, or the system, satisfy any safety integrity requirements.

Direct Evidence

Direct evidence usually consists of the following categories:

- Analysis evidence
- Demonstration evidence
- Quantitative evidence
- Review evidence
- Qualitative evidence

Analysis Evidence

Evidence from the analysis is used to demonstrate absence of dangerous faults and achievement of requirement. It may also be used to derive requirements and to provide evidence of the types of failure mode that are possible (or prevented from occurring). Reasonable justification should be provided for the context and limitations of the evidence generated by the analysis. The analyses should be fully documented, and work products should be held under configuration control, so that the analyses are repeatable, auditable, and verifiable. Justification for the competence of the skills of the people performing the analyses is required, as well as for the accuracy, validity, and appropriateness of the processes and tools used.

The models used in the analyses should be justified and evidence provided for the correctness and suitability of the model. All analyses are dependent on some form of model (e.g., how source code is translated into an executable form on a particular processor). Computational modeling techniques rely on underlying probability distribution models (e.g., for the accuracy and sensitivity to error), and they should provide justification of the selection and appropriateness (or sensitivity) of the model or technique.

Demonstration Evidence

Operational experience, verification, and validation evidence is used to demonstrate that the behavior of the system is safe. If demonstration evidence forms part of the railroad's argument that the functional requirements have been satisfied, verification and validation of dynamic behavior should be fully documented, and work products should be held under configuration control, so test cases are repeatable, auditable, and verifiable. The extent and coverage of dynamic behavior through verification and validation or operational experience should be justified. The differences between any test environments and the operational environment should be documented. Demonstration evidence is necessary to show that the test environment and test cases provide a valid demonstration of operational behavior.

The demonstration evidence may come from testing or from exercising the system in an operational context and the detailed evidence may be further analyzed to form quantitative evidence. Requirement-based testing generally produces evidence that is easier to link to safety claims. The test cases for empirical testing (black box) may be based on a risk assessment of the outputs, specified functional requirements, error guessing, known problem areas, etc. The test program should be representative of the operational environment (e.g., in designing the test environment and test cases). The extent and coverage of the testing

executed needs to be commensurate with the requirements. A risk-based approach to testing is recommended, understanding the purposes, strengths, and weaknesses of the proposed test method and extent of testing.

For operational experience, it will be necessary to examine whether unusual or abnormal conditions have been exercised. Simulated experience or testing may be necessary if this is not the case.

Quantitative Evidence

Quantitative evidence is used to show how the system performs against its quantitative requirements. Quantitative analyses should be fully documented and the output and data used should be held under configuration control, so that the quantitative analyses are repeatable, auditable, and verifiable.

The confidence levels from the quantitative analyses should be stated and justified. Quantitative evidence should be of the same quality as the requirements. Quantitative evidence usually relies on statistical models. One should ensure that the model used is appropriate and the results are relatively insensitive to the assumptions (or provide further evidence to show that the assumptions are valid). Quantitative evidence (e.g., reliability or availability) may be generated from statistical testing or inservice history. Predicted reliability may be analyzed from failure free models, distribution models based on numbers of faults seen, or reliability growth models. These techniques are more practicable for systems with modest quantitative requirements.

When quantitative evidence is generated from pre-operational testing, the test cases (or software used to generate test inputs) should be held under configuration control. When the quantitative data is derived from operational experience, it may be impracticable to retain the actual data. Evidence of the nature of the operational profile and performance (e.g., from operators' logs or data analysis) should be retained. It may be necessary to discuss the provisions of operational and inservice data with the railroad and vendor.

There will be some systems where the risk is very low (i.e., broadly acceptable). For such systems, it will not be necessary to expend significant effort in demonstrating that quantitative requirements are met.

When the quantitative evidence is used as a primary argument, the process requirements and quantitative criteria to be used for the continuous collection and analysis of such evidence during operational use must be documented. Requirements specified should include quantitative requirements or all the quantitative properties of the system that are relevant to system functionality (such as probability of dangerous failure, unavailability, timeliness, robustness, capacity). The system should also satisfy its quantitative functional requirements (i.e., quantitative evidence from actual or realistic operation of the complex electronic element is provided).

Review Evidence
Review evidence is used to show that the system is capable of satisfying its safety requirements. The review evidence must cover:

- Traceability, to ensure that safety requirements are translated into the derived safety requirements, and therefore into the implementation,
- Maintainability, where required as part of the safety requirements, to ensure that the complex electronic element is designed in a way that facilitates future modification or correction.
- Compliance, to ensure that design and implementation practice conforms with specified standards of good practice.
- Validity, to ensure that the complex electronic element implements the safety requirements and does so correctly (verification).
- Robustness, to ensure that faults in the complex electronic element, as well as failures originating in other system elements, are managed safely.

Qualitative Evidence
Qualitative evidence is used to show that good practice has been used in the selection of derived requirements, architecture, and design features of the system. Qualitative evidence of good design should be provided for all necessary features and requirements. The evidence should include the rationale, benefits, and limitations of the design. Evidence of good design should include references to significant examples or case studies illustrating successful use, where available. Evidence should be provided that this design is appropriate, given the system context and the functionality and safety-related roles.

In general, qualitative evidence provides secondary arguments that support other, stronger forms of evidence (such as quantitative evidence and demonstration evidence). These qualitative arguments will help future maintainability by helping to draw attention to the features and properties that matter. The absence of such qualitative arguments might cause a reviewer to doubt whether good practice had been used; therefore, undermining confidence in the system.

In the case of many of the functions, good design will be implicitly demonstrated by an analytical or quantitative analysis that demonstrates the effectiveness of that feature. In such cases, qualitative arguments would add very little. However, qualitative arguments may be provided where the effort to conduct such an analysis would be excessive or the analysis would be impracticable. A qualitative argument may be all that can be provided where it is difficult to determine the individual contribution of specific features to the overall performance of the complex electronic element (e.g., using a modular architecture may be cited as good design, but it is difficult to determine how much a modular architecture contributes to the safety integrity).

Process Evidence

Process evidence should support the direct evidence. For all systems (including off-the-shelf and existing systems with a poorly documented development history), process evidence should encompass all assurance and risk assessment and risk mitigation processes, including

hazard analysis, system selection, integration, commissioning, and modification processes. For newly developed systems and existing systems with a well-documented development history, process evidence will also include the development and maintenance processes.

Process Description and Rationale
A description and risk-based rationale of the processes should be provided. This process description and rationale should show that a risk-based approach is used to minimize introduction of safety significant faults and maximize detection and correction. For low integrity systems, the process description may be little more than an explanation of the activities, the potential errors and how these will be detected. For higher integrity systems, process metrics may be used to demonstrate that effort is concentrated where errors are more likely or more serious. For the highest integrity systems, the process evidence should demonstrate, so far as reasonably practicable, the absence of dangerous faults.

Where off-the-shelf or other existing systems or subsystems are used, it should detail the processes used for evaluation, validation, and implementation of the system, the processes used for any associated software or hardware (such as software wrappers or hardware interlocks) and any information from the supplier about the development process. In general, the more onerous the safety integrity requirements, the more rigorous and compelling the process evidence that should be provided. For an off-the-shelf or preexisting element, the rigor may have to be provided at the evaluation stage.

Process and Tool Qualification
Evidence should be provided to show that the tools and processes used have sufficient safety assurance to guarantee that they will not undermine the integrity of the development of the complex electronic element. The competence requirements for personnel undertaking each process should be stated, and the information should be retained regarding the competence of the personnel performing the processes. Each tool and process should be evaluated to determine its role and significance to safety. The following list is specific to safety issues; however, this is not an exhaustive list of factors relevant to tool selection (others may include usability, interoperability, stability, commercial availability, maintenance support, familiarity to safety personnel, etc.):

- The role of the tool or process in assuring the safety.
- Whether the tool or process could introduce a safety significant fault.
- Whether the tool or process could fail to detect a safety significant fault.
- How failures of the tool or process could be detected and corrected by human supervision and by other tools and processes.

A risk-based justification for the use of the tool or process should be produced and supported by evidence for its suitability, which may include:

- Procedures that provide safeguards against tool or process failures.
- Previous experience of use of the tool or process (in other systems).
- Analyses and test results.
- Current experience in the application of the tool or process (e.g., in the assurance of this system).

The evidence for the processes and tools actively used for the maintenance and modification of complex electronic elements should be kept up to date and be periodically reviewed to consider changes in the consensus on good practice.

Good Development Practice
Evidence should be available to verify that the processes used in the risk assessment, procurement, development, implementation, verification, validation, modification, and correction of the system all conform to good practice. The evidence of good practice should be appropriate to the application, domain, and safety requirements. Examples of good practice in process include:

- Evidence of compliance with appropriate, respected standards—preferably standards that are international, relevant to the domain and mature, but still considered good practice.
- Evidence of selection of good practice methods, tools, technology, etc. (this will typically be at a more technical level of detail than is covered by an international standard and may include specific software language, hardware technology, development toolsets, etc.).
- Evidence of applying good practice in methods, technology, tools, etc. (e.g. internal procedures, processes, and standard tool supplier's recommended best practice, user group recommendations, etc.).

Process Effectiveness and Repeatability
Evidence should be provided that verifies that the processes used for the risk assessment, procurement, development, implementation, verification, validation, modification, and correction of the system are repeatable and effective. Processes should provide for some form of double check to avoid single points of failure, sensitivity of the process to human error, and individual differences in expertise. A single individual may make errors in judgment, and therefore, consensus techniques, including peer review, should be used. The higher the integrity, the greater the rigor and level of double checking that is required. Where possible, process measurement (metrics) should be used to demonstrate the repeatability and effectiveness of processes.

Error Detection, Sentencing, and Change Management
Evidence should be provided to show that processes for the detection and correction of errors are effective and tend to increase the integrity of the system. Disposition (i.e., sentencing) is the process of determining the impact and risk arising from an identified fault and, therefore, in determining and prioritizing corrective action. Disposition may include the decision that no action is required. Realistically, changes and error correction will form a part of any significant project. The evidence should show that errors are detected, correctly sentenced, and suitably corrected. For high integrity systems, if errors are found during processes intended to confirm absence of faults (such as statistical testing), additional justification should be provided for claims for low fault density.

Counter Evidence

Counter evidence will almost certainly be created in the development of a complex electronic system (e.g., from failed tests, faults found during review, etc.). Off-the-shelf systems are also likely to have experienced failures and counter evidence may include problems during commissioning, lists of known faults from suppliers, and experience from user groups. Evidence should be provided to show that sources of potential counter evidence, including test evidence, insecurities in development processes, inservice history and experience with other similar systems have been scrutinized.

Counter evidence should be documented, analyzed, and referenced to the affected safety requirement. The analysis of counter evidence should include:

- Assessment of the potential impact of the problem on the safety of the system.
- Determination of corrective action, if appropriate, including verification of actions and analysis of effectiveness.
- Assessment of the origin and underlying causes of the problem.
- Assessment of the effect of the counter evidence on the safety claims.

Counter evidence has the potential to be stronger than positive evidence for safety. Even identification of a single, potentially dangerous fault or a single failure during operation or testing may be sufficient to invalidate the safety case. However, after analysis, it may be the case that the majority of counter evidence consists only of minor deviations that do not significantly affect the safety arguments.

While counter evidence has the potential to refute the safety claims, a rigorous search for counter evidence and its objective analysis is evidence of a robust safety management process. The absence of documented counter evidence might be indicative of an inadequate Safety Management System. Counter evidence includes:

- Inservice incidents: Performance of failure management procedures and systems as well as the origin, sentencing, and correction of faults.

- Inherent insecurities or weaknesses in processes: Steps taken to ensure issues such as insecurities in coding languages, layout issues in hardware design, processes subject to human error have not had an adverse effect on safety in the complex electronic element.

- Fault detection, sentencing, retest/reanalysis/re-review: Evidence of fault detection, diagnosis, sentencing, correction, and confirmation of correction (e.g. failed test results, change documentation) and metrics of faults.

Sufficiency and Composition of Evidence

The body of evidence, taken as a whole, should be sufficient to provide confidence, commensurate with the requirements, in the safety of the system. For off-the-shelf or legacy systems, it may be impracticable to generate certain types of evidence (e.g., because of lack of white box visibility (has all information available and access to development process

data)). If proposing to use off-the-shelf or legacy elements, the railroad should have ensured that it is possible to produce sufficient evidence to support the safety claims.

The primary arguments for system acceptance should be based on direct evidence, which may include analysis evidence, demonstration evidence, review evidence, and quantitative evidence. Process evidence should be used to support the primary arguments (and may additionally support claims for future maintainability if this is a safety concern within the safety case). Qualitative evidence for good design should support the other forms of direct evidence. It is unlikely to generate sufficient quantitative data to support a quantitative safety claim to the required statistical confidence during the development phase of complex electronic elements with high safety integrity requirements. In these cases, an argument based on diverse direct evidence should be used to drive the design of the complex electronic element.

Strength and Rigor of Evidence

The rigor of the evidence and arguments should be proportionate with the required level of safety. The type of evidence provided for primary arguments should be based on the precedence below (preferred first). The primary safety arguments should be based on the strongest types of evidence and then supported by other types of evidence.

- Analysis evidence for the absence of dangerous faults, the satisfaction of safety requirements and the implementation of derived safety requirements.
  - For complex electronic elements, whose quantitative safety requirements exceed those that can be quantitatively demonstrated to a level of confidence commensurate with the safety integrity requirements at entry into service. The primary arguments should be based on rigorous, analytical evidence for the absence of dangerous faults and the achievement of the derived safety requirements.

- Quantitative analysis of operational or realistic demonstration of the required behavior that shows that availability and reliability requirements are satisfied, to a level of confidence commensurate with the safety integrity requirements of the system.
  - Quantitative evidence should be provided for all complex electronic elements, even if it is not practicable to demonstrate to a sufficient confidence the satisfaction of the quantitative requirements.

- Demonstration evidence and review evidence.
  - Safety claims based solely on black box, empirical demonstration evidence should generally only be used for elements with low safety integrity requirements where failures of the complex electronic element are managed by other system elements.
  - Review evidence is more compelling if supported by metrics that demonstrate the effectiveness of the review processes.

- Qualitative evidence of good design, and process evidence.
  - Qualitative evidence should be provided for all complex electronic elements. However, safety claims based solely on qualitative evidence should only be used for elements with low safety integrity requirements, where failures of the complex electronic element are managed by other system elements.
  - Process evidence should be provided for all complex electronic elements (e.g., for off-the-shelf and legacy systems) even if the processes only relate to evaluation and integration. However, some form of direct evidence should always be provided. Good processes (such as those defined by international standards) will tend to generate direct evidence such as review evidence and demonstration evidence from testing.

Coverage of Evidence

The evidence provided should be representative of all aspects of the argument that it supports and sufficiently extensive to provide the required level of confidence. This requires that the evidence should support safety requirements and derived safety requirements. The assumptions, dependencies, and limitations of the evidence for all safety claims should be documented. Analysis evidence should be supported by diverse demonstration evidence. Quantitative evidence should be supported by at least diverse traceability evidence and evidence from review of architecture and implementation quality.

Several arguments may be needed to cover different aspects of a safety claim. In particular, additional evidence should be provided to show that the observed behavior is representative of the actual operational behavior where evidence is derived from, such as:

- An artificial environment.
- Execution of only a part of the system
- A theoretical model.

The limits of coverage of the evidence should be identified; for example, where only part of the implementation is formally analyzed, or testing is less than 100 percent implementation coverage, or sampling is used in review.

Scrutiny of Evidence

Evidence should be provided of independent verification and assessment of evidence, arguments, and safety claims. Evidence of scrutiny includes audit reports, corrective action etc., as well as quality assurance and verification and validation documentation such as peer review. The goal-based approach to safety assurance means a larger scope for the railroad and vendor to exercise flexibility in approach; therefore, more emphasis is needed on independent scrutiny and assessment. Consequently evidence required for assurance is detailed and extensive. Therefore, the effort required for adequate scrutiny of evidence is also likely to be significant.

For each piece of evidence (the generating process), it should be checked by a different person than the one who originated the evidence and preferably part of a different team (e.g.,

a safety team separate from the operational users, or a verification and validation team separate from a development team). Where the scrutiny involves significant judgment, i.e., independent audit and assessment, an independent and separate organization should be used. For the highest integrity systems and for safety critical single points of failure, the checking process should be detailed with the result that there is 100 percent scrutiny of the evidence and evidence generating processes.

For lower integrity systems, a sampling approach using less than 100 percent coverage may be used. The level of sampling should be proportionate to the risk and the findings of the sampling. If problems with the evidence are discovered, more extensive verification, audit, and assessment should be undertaken. Some of the evidence of independent scrutiny may derive from activities performed. Independent assessment of safety claims and arguments may be performed.

Audit Checklist

Audit checklists focus the auditors on critical attributes that the railroad's processes and procedures must address. They also, when considered in the context of the evidence presented, allow the auditor to reduce the degree of subjectivity when evaluating the functional testing and draw fairly based conclusions about the extent to which the data supports the railroads argument that the required functionality has been provided.

Audit checklists also provide a mechanism for the regulator to identify critical performance concerns of the regulated entity and provide a baseline for the regulated entity to develop those appropriate processes and procedures. The checklist in Appendix A should be used to facilitate and provide guidance for the evaluation of the railroad's functional testing efforts. The checklist has been created primarily considering general situations and is independent of the specific types of evidence. Particular projects may have other unique project requirements, and the checklist in Appendix A should be tailored to make it more effective and efficient. Keep in mind that the main idea is that there should be a systematic review of requirements based on a checklist that makes sense for your project

Virtually all elements associated with the checklist in Appendix A require written plans, processes, procedures, and polices There are differences that must considered when evaluating compliance with the audit requirements. Policy is set of ideas or a plan of what to do in particular situations that has been officially agreed on. A plan is a detailed proposal for doing or achieving something. Plans implement policy. It identifies the various processes required. A process defines what needs to be done, and the various roles that are involved. It outlines the roles and responsibilities of the people assigned to do the work, the appropriate tools and equipment to support individuals in doing their jobs, the procedures and methods defining how to do the tasks, and the relationships between the tasks. A procedure defines how to do a task and is usually associated with a subset of the roles involved.

This checklist should not be used in a "yes/no" manner, always remembering that different evidence may be presented for the different functions. The idea is to consider what might be possible, and then determine what is feasible. The checklist should be reviewed periodically.

Users of this checklist may find it helpful to rephrase questions in order to prompt maximum creativity; for example "how might it be possible to...?" This checklist does not take the place of the manufacturer's recommended checkout and startup procedures or report.

Coordination and Scheduling

The railroad shall provide sufficient notice to FRA regarding their completion schedule for the pre-functional testing of all equipment and systems. FRA may choose not to attend the testing. As is the case with other regulatory requirements, responsibility for compliance is with the railroads. The railroad retains ultimate responsibility not only for their actions, but also for the actions of their contractors and subcontractors. Functional testing shall be conducted only after all pre-functional testing has been completed to FRA's satisfaction.

Testing proceeds from components to sub-systems to systems. When the proper performance of all interacting individual systems has been achieved, the interface or coordinated responses between systems shall be checked. The functional testing shall demonstrate that each system is operating according to the documented design intent and contract documents. Functional testing facilitates bringing the systems from a state of individual substantial completion to full dynamic operation. Additionally, during the testing process, areas of deficient performance are identified and corrected, improving the operation and functioning of the systems.

Before test procedures are finalized, the railroad must provide FRA all requested documentation and a current list of changes affecting equipment or systems, including an updated points list, program code, control sequences, and testing parameters. Using the testing parameters and requirements in the technical specifications, the railroad must update or develop specific test procedures and forms to verify and document proper operation of each piece of equipment and system. The railroad must provide a copy of the test procedures to FRA no less than 10 working days prior to the commencement of the proposed start of testing. FRA shall review the tests for feasibility, safety, equipment, and protection. The final test forms must be submitted to FRA for formal review and approval.

Failures

If 10 percent (or three, whichever is greater) of the identical pieces (size alone does not constitute a difference) of equipment fail to perform to the requirements (mechanically or substantively) due to a defect not allowing it to meet its submitted performance specification, all units will be considered unacceptable by FRA. In such case, the railroad must:

- Stop all testing.
- Within 1 week of identification, examine all other identical units, making a record of the findings. The findings shall be provided to FRA within 2 weeks of the original notice.
- Within 2 weeks of the original notification, provide a signed and dated written explanation of the problem, cause of failures, all proposed solutions, etc. The

proposed solutions must not significantly exceed the specification requirements of the original installation.

- The railroad shall replace or repair all identical items at their expense. The replacement or repair work shall proceed with reasonable speed beginning within 1 week from when parts can be obtained. Testing may resume upon FRA notification of the completed repairs.

Appendix A: Audit Checklist

Each function and test shall be performed under conditions that simulate actual conditions as close as is practically possible. The railroad executing the test shall provide all necessary materials, system modifications, etc., to produce the necessary flows, pressures, temperatures, etc., necessary to execute the test according to the specified conditions. At the completion of the test, the railroad must return all affected equipment and systems to their normal operating condition.

Audit Element	Audit Attribute	Y	N	Comments
1.	The railroad has identified senior railroad management staff (mechanical, signal, operating, track, and IT personnel) ultimately accountable for testing in writing.			
2.	The railroad has specified in writing, the responsibilities of all railroad personnel (management, mechanical, signal, operating, track, and IT personnel) involved in the testing.			
3.	The railroad has a current organizational chart that shows the relationship between railroad personnel involved with system development and maintenance.			
4.	The railroad has specified in writing the responsibilities of all vendor personnel (management, mechanical, signal, operating, track, and IT personnel) involved in the testing.			
5.	The railroad has a current organizational chart that shows the relationship between vendor personnel and the railroad personnel involved with system development and maintenance.			
6.	The purpose of each of the test results and evaluations has been described.			
7.	The scope of the test results and evaluations has been described.			
8.	The system or project under test has been described.			

9.	The function under test has been traced to one or more system requirements.			
10.	The test baseline configuration has been determined.			
11.	The test start and end dates have been defined.			
12.	The number of personnel to conduct the test has been defined.			
13.	The required resources to conduct the test are available.			
14.	The system test environment has been described.			
15.	The required test resources have been identified and are in hand.			
16.	Is the required data available?			
17.	How will the test data be identified and maintained?			
18.	The type of test has been identified • Unit • Functional • Load • Volume • Acceptance • Compatibility • Conformance • Stress • Vulnerability • Regression			
19.	The test entry conditions have been defined.			
20.	Have the expected results and test exit results been defined?			
21.	The test can be performed as written.			
22.	If the test cannot be performed as written, have the procedures been redlined, with redlines incorporated into the master test document?			
23.	Have the performance results of the test been quantifiably defined?			
24.	Are the performance results from testing consistent with expected test results?			

25.	Are the performance results consistent with design requirements?			
26.	The security requirements for the system have been defined and implemented.			
27.	Have problems been entered in the Change Request Tracking Database?			
28.	The railroad has identified, in writing prior to each test, the status of each outstanding discrepancy identified, covering explanations of any disagreement and proposals for their resolutions.			
29.	The system successfully tested using randomly generated inputs within the typical test range.			
30.	The system successfully tested using boundary data to check robustness of the program. This also includes testing for null or zero values.			
31.	The system successfully overloaded to see where it reaches its maximum capacity.			
32.	A procedure exists for handling emergency changes that cannot be implemented as part of a scheduled release.			

33.	Have all sources of risks been identified? • Technical (e.g., new detectors do not perform as expected) • Institutional (e.g., agency data sharing, new regulations, public opposition) • Funding (delays or cuts) • Environmental (e.g., temperature levels for outdoor field equipment, restrictions on building) • Personnel (e.g., loss of key personnel, substandard performance) • Commercial (e.g., vendor does not deliver off-the-shelf product)			
34.	Were experts and stakeholders queried in all the areas to develop a broad list of credible risks?			
35.	Are the risks prioritized and the most critical ones identified?			
36.	For each high priority risk, are there ways to eliminate the risk? Or, reduce its likelihood or impact?			
37.	For each high priority risk, have the symptoms of the problem and a means for monitoring them been identified?			
38.	Are the high priority risks regularly monitored throughout the project?			
39.	For each high priority risk, is there a risk resolution plan?			
40.	Is access to the requirements management tool available to all stakeholders and the development team?			
41.	Has the extent of traceability been defined?			
42.	Are all user needs or requirements traced to system requirements?			

43.	Have the concept of operation scenarios been traced to the system requirements and the validation plan?			
44.	Have the system requirements been traced to the system verification plan?			
45.	Have the system requirements been traced to the high level design?			
46.	Has the high level design been traced to the sub-system verification plans?			
47.	Has the high level design been traced to the detailed design?			
48.	Has the detailed design been traced to the unit verification plan or procedures?			
49.	Has the detailed design been traced to implementation artifacts (SW source code, HW documentation, etc.)?			
50.	Have the verification procedures been traced to the verification plans at all levels?			
51.	Has all needed supporting project documentation been traced?			
52.	Has traceability been maintained during the operations and maintenance, changes and upgrades, and retirement and replacement?			
53.	Is there a documented verification plan for the project?			
54.	Does the verification plan answer all the questions of who, what, where, and when concerning test conduct?			
55.	Does the verification plan make clear what needs to happen if a test failure is encountered?			
56.	Does the verification plan define the configuration of the hardware, software, and external system needed for each test case?			

57.	Are all applicable requirements traced to a test case in the verification plan? Does each test case define a realistic and doable test?			
58.	Are detailed verification procedures documented for the project?			
59.	Is each step in the verification procedure traced to a test case and a requirement?			
60.	Are all of the necessary initial conditions and setup defined for each procedure?			
61.	Has each verification procedure been through a dry run prior to the formal test? Have the procedures been updated as a result?			
62.	Is there a verification report that documents the project verification results?			
63.	Does the verification report describe, in detail, the resolution of every test anomaly encountered during testing?			