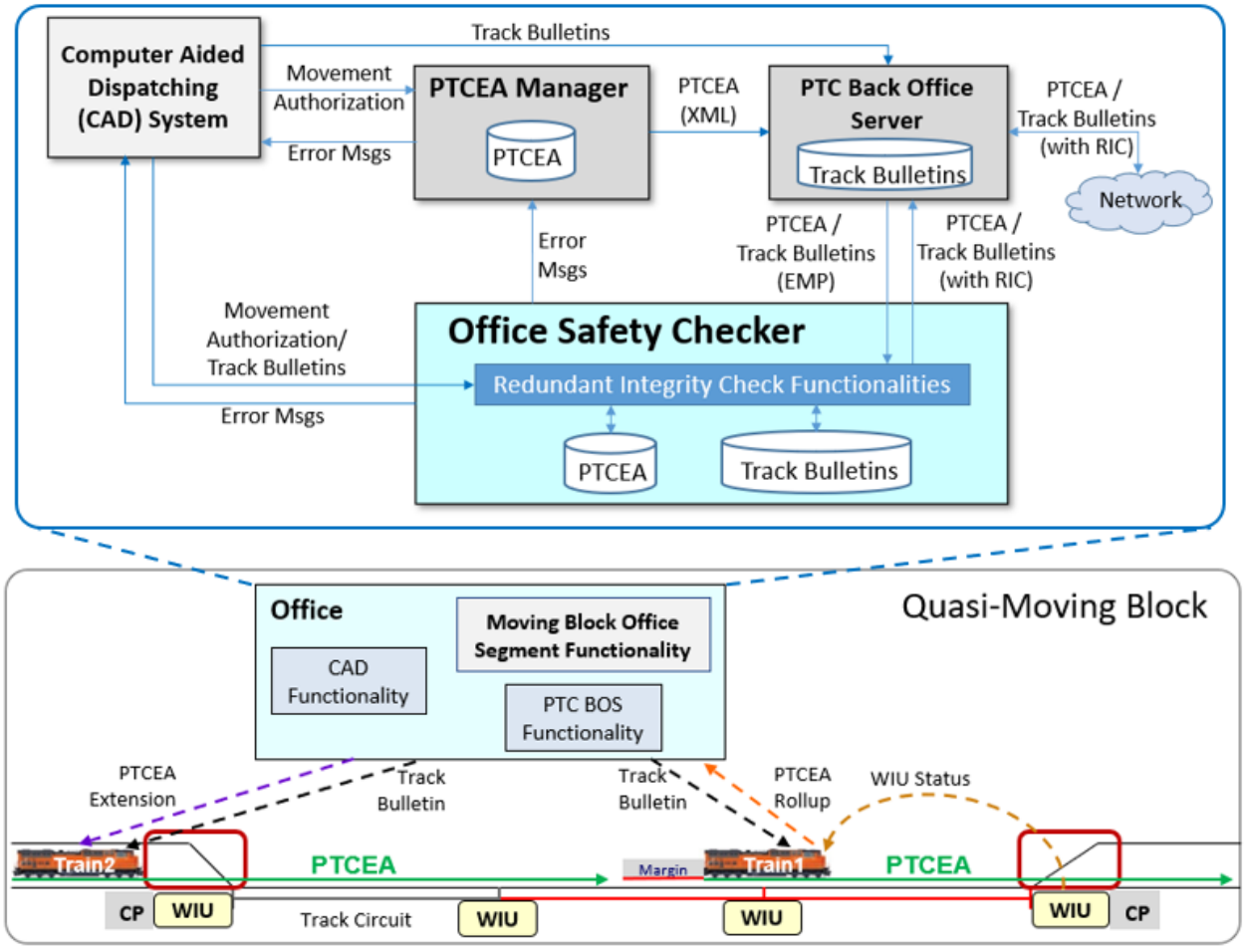
U.S. Department
of Transportation
Federal Railroad
Administration

Office of Research,
Development and Technology
Washington, DC 20590

Office Safety Checker for Moving Block Train Control Systems



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-05-2022	Technical Report	6/26/2020 – 5/10/2022

4. TITLE AND SUBTITLE
Office Safety Checker for Moving Block Train Control Systems

5a. CONTRACT NUMBER
DTFR53-11-D-00008L

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Jose Rosales - 0000-0001-6825-3010
Paulo Viera - 0000-0002-3617-9490
Alan Polivka - 0000-0002-6424-5846

5d. PROJECT NUMBER

5e. TASK NUMBER
693JJ20F000036

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Transportation Technology Center, Inc.
55500 DOT Road
PO BOX 11130
Pueblo, CO 81001-0130

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Department of Transportation
Federal Railroad Administration
Office of Railroad Policy and Development
Office of Research, Development, and Technology (RD&T)
Washington, DC 20590

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
DOT/FRA/ORD-23/28

12. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the FRA Web site at http://www.fra.dot.gov

13. SUPPLEMENTARY NOTES
COR: Jared Withers

14. ABSTRACT
As part of a project sponsored by the Federal Railroad Administration (FRA), Transportation Technology Center, Inc., (TTCI), developed and analyzed a concept for the Office Safety Checker (OSC) component of the Moving Block Office (MBO), a segment of a moving block train control system concept. The OSC component performs a safety validation of MBO safety-critical functions and certain Positive Train Control Back Office Server (PTC-BOS) safety-critical functions. It also leverages on the Quasi-Moving Block (QMB) Operational Concept and the Overlay Positive Train Control (O-PTC) concepts.

15. SUBJECT TERMS
Office Safety Checker (OSC), Quasi-moving block (QMB), Full Moving Block (FMB), Interoperable Train Control (ITC), Positive Train Control (PTC), Centralized Interlocking (CIXL)

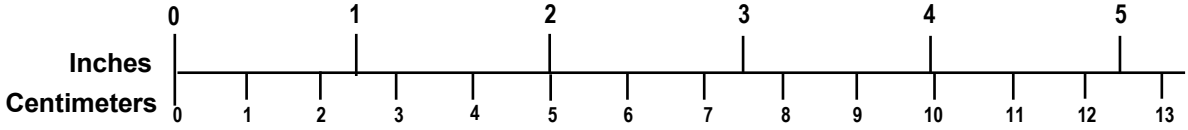
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jose Rosales
Unclassified	Unclassified	Unclassified		139	19b. TELEPHONE NUMBER *(Include area code)* 719-584-0561

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

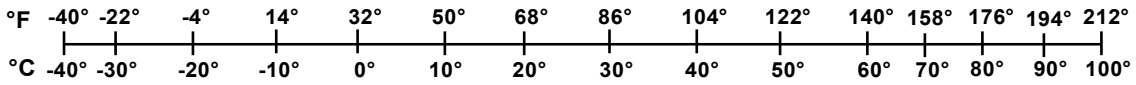
METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC	METRIC TO ENGLISH
LENGTH (APPROXIMATE)	**LENGTH (APPROXIMATE)**
1 inch (in) = 2.5 centimeters (cm)	1 millimeter (mm) = 0.04 inch (in)
1 foot (ft) = 30 centimeters (cm)	1 centimeter (cm) = 0.4 inch (in)
1 yard (yd) = 0.9 meter (m)	1 meter (m) = 3.3 feet (ft)
1 mile (mi) = 1.6 kilometers (km)	1 meter (m) = 1.1 yards (yd)
	1 kilometer (km) = 0.6 mile (mi)
AREA (APPROXIMATE)	**AREA (APPROXIMATE)**
1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)	1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m^2)	1 square meter (m^2) = 1.2 square yards (sq yd, yd^2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)	1 square kilometer (km^2) = 0.4 square mile (sq mi, mi^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)	10,000 square meters (m^2) = 1 hectare (ha) = 2.5 acres
1 acre = 0.4 hectare (he) = 4,000 square meters (m^2)	
MASS - WEIGHT (APPROXIMATE)	**MASS - WEIGHT (APPROXIMATE)**
1 ounce (oz) = 28 grams (gm)	1 gram (gm) = 0.036 ounce (oz)
1 pound (lb) = 0.45 kilogram (kg)	1 kilogram (kg) = 2.2 pounds (lb)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)	1 tonne (t) = 1,000 kilograms (kg)
	= 1.1 short tons
VOLUME (APPROXIMATE)	**VOLUME (APPROXIMATE)**
1 teaspoon (tsp) = 5 milliliters (ml)	1 milliliter (ml) = 0.03 fluid ounce (fl oz)
1 tablespoon (tbsp) = 15 milliliters (ml)	1 liter (l) = 2.1 pints (pt)
1 fluid ounce (fl oz) = 30 milliliters (ml)	1 liter (l) = 1.06 quarts (qt)
1 cup (c) = 0.24 liter (l)	1 liter (l) = 0.26 gallon (gal)
1 pint (pt) = 0.47 liter (l)	
1 quart (qt) = 0.96 liter (l)	
1 gallon (gal) = 3.8 liters (l)	
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)	1 cubic meter (m^3) = 36 cubic feet (cu ft, ft^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)	1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)
TEMPERATURE (EXACT)	**TEMPERATURE (EXACT)**
[(x-32)(5/9)] °F = y °C	[(9/5) y + 32] °C = x °F

QUICK INCH - CENTIMETER LENGTH CONVERSION



QUICK FAHRENHEIT - CELSIUS TEMPERATURE CONVERSIO



For more exact and or other conversion factors, see NIST Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50 SD Catalog No. C13 10286

Updated 6/17/98

Contents

Executive Summary 1

1. Introduction 3
   - 1.1 Background 3
   - 1.2 Objectives 3
   - 1.3 Overall Approach 3
   - 1.4 Scope 4
   - 1.5 Organization of the Report 4

2. Project Overview 5
   - 2.1 OSC ConOps 5
   - 2.2 OSC SegRS 6
   - 2.3 OSC Safety Analyses 6

3. Conclusions 8

4. References 9

Appendix A. Concept of Operations 10

Appendix A-1. CIXL Operation Scenarios 60

Appendix B. Segment Requirements 66

Appendix C. Safety Analysis 106

Abbreviations and Acronyms 130

Illustrations

Appendix A

Figure 1. Schematic of Typical CTC Territory 15
Figure 2. High-level Architecture of ITC (O-PTC) System 17
Figure 3. Wayside Signal Aspects and WSMs in Overlay PTC and EO-PTC 18
Figure 4. Onboard Display in EO-PTC 18
Figure 5. QMB Functional Architecture Diagram 19
Figure 6. QMB Functional Architecture with Field Interlocking 20
Figure 7. QMB Architecture with CIXL 20
Figure 8. OSC High-Level Functional Architecture Diagram showing Two Different Interlocking Approaches 26
Figure 9. OSC Architectural Design with Diversity and Self-Checking SAC Principle 28
Figure 10. Alternative Architectural Design with N-version Programming SAC Principle 30
Figure 11. MBO Core Architecture with OSC 32

Appendix C

Figure 1. Hazard Risk Index 113

Tables

Appendix A

Table 1. QMB Expected Benefits 22

Table 2. Movement Authority ITC PTC Messages 34

Table 3. Authority Rollup ITC PTC Messages 34

Appendix B

Table 1. List of Configurable Parameters 102

Table 2. List of Event Reports 102

Appendix C

Table 1. Summary Results of the OSC Safety Analysis 116

Table 2. Hazard Risk Assessment Results 117

Executive Summary

Transportation Technology Center, Inc. (TTCI) conducted a research project for the Federal Railroad Administration (FRA) with the goal of developing system engineering documents for an Office Safety Checker (OSC) system component, a component that is part of the Moving Block Office (MBO) that performs both Quasi-Moving Block (QMB)- and Full Moving Block (FMB)-specific functions in the Office. During the project's period of performance of June 2020 to May 2022, TTCI collaborated with a railroad technical advisory group (TAG) to develop concepts and key design details and prepare a safety analysis that will support the future development and deployment of the OSC, a system component that supports the MBO, and the Positive Train Control (PTC) Back Office Server (BOS) system segments.

In comparison with fixed-block Overlay PTC (O-PTC) systems, the FMB train control system concept offers improvements in both safety and operations. Safety can be improved by providing collision protection at restricted speeds, as well as other speeds. Operational improvements can be made by eliminating the constraints of fixed-block track circuits and allowing shorter headways, thereby increasing traffic capacity. The FMB requires an alternative to fixed-block track circuits to detect rail breaks and rollouts (unauthorized track occupancies). Since no such detector is currently available, the QMB has been conceived as a hybrid system that incorporates features of both fixed-block and FMB train controls to allow implementation with the current technology. Specifically, QMB achieves restricted speed collision protection and a portion of the FMB operational benefits (in certain implementations), while using fixed-block track circuits.

In QMB or FMB train control systems, messages containing PTC Exclusive Authorities (PTCEAs) and track bulletins are delivered electronically and may be the sole artifacts, besides track status information (including civil speed restrictions), that crews depend on for safe train operation. Therefore, the data within these messages and the functions that generate them are considered safety critical and require validation for the safety of rail network operations. The OSC comprises the set of office functions that implements this safety validation for Moving Block and PTC operations.

The team developed the system engineering documentation that defines the OSC component. The first product of the project is a comprehensive OSC Concept of Operations (ConOps) document that was leveraged from the QMB ConOps and O-PTC concepts. The proposed concept for the OSC functions is based on the federal requirements regarding safety assurance criteria and processes found in 49CFR236 Subpart I, Appendix C [1], referring to Safety Assurance Concepts (SAC) to achieve a fail-safe implementation. The SAC are defined in the IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control (IEEE-1483-2000) [2].

The Diversity and Self-Checking SAC were adopted for the development of the OSC requirements, as well as applied collectively to the PTCEA Manager, PTC-BOS, and OSC segments. These segments work with the PTC onboard segment such that each safety-critical office function performed by the PTCEA Manager or PTC-BOS, or the result thereof, is checked for correctness by the OSC and PTC onboard segment before action is taken. Critical OSC components also perform internal self-checking.

The proposed OSC architecture is advantageous for the following reasons:

- It reduces the vitality of minimum functions when used in conjunction with a fail-safe onboard segment that verifies Cyclic Redundancy Checks (CRCs) and Hash-based Message Authentication (HMAC) applied by diverse office systems.
- It contains the entire OSC in a single environment.
- It is decoupled from functions that implement business functions (such as Computer-Aided Dispatch (CAD) Movement Authority (MA) parsing or CAD interface functions) that do not necessarily need a fail-safe implementation.
- A loose coupling with other office components allows for full reuse of a railroad's existing PTC-BOS without requiring the OSC to access any interfaces that are internal to the PTC-BOS.

The second product of the project is the OSC Segment Requirements Specification (SegRS) document that includes functional and non-functional requirements. This document is leveraged from the QMB system and segment requirements and includes the necessary modifications and additions required for OSC implementation.

The third product is the OSC safety analysis that includes 1) the MBO hazards associated with safety-critical functions, 2) the PTC-BOS hazards associated with functions that handle messages that include safety-critical information sent from the office to trains, and 3) the risks associated with these types of hazards. This analysis also describes how these hazards can be eliminated or mitigated with the implementation of an OSC and concludes that the risks can be mitigated to an acceptable level by implementing it to safely validate the office functions considered safety critical for both QMB and FMB operations. The OSC safety analysis produced in this project is a preliminary draft that will require further updates by any railroad choosing to implement a QMB system (including OSC) to account for railroad-specific characteristics.

1. Introduction

Transportation Technology Center, Inc. (TTCI) conducted a research project for the Federal Railroad Administration (FRA) with the goal of developing system engineering documents for an Office Safety Checker (OSC) system component that will support Quasi-Moving Block (QMB) and Full Moving Block (FMB) methods of train control, defined under the Higher Reliability and Capacity Train Control (HRCTC) program. During the period of performance of the project (June 2020 to May 2022), TTCI developed a Concept of Operations (ConOps), a Segment Requirements Specification (SegRS), and a Safety Analysis for the OSC.

1.1 Background

As part of the HRCTC program, the team has identified and researched new methods of train control that have the potential to enhance railway safety, reliability, and operational performance leveraging Positive Train Control (PTC) technology. Three new modes of train control, referred to as Enhanced Overlay PTC (EO-PTC), Quasi-Moving Block (QMB), and Full Moving Block (FMB), have been identified as the logical evolution from the Interoperable Train Control (ITC) form of PTC currently in production, herein identified as Overlay PTC (O-PTC).

One of the core concepts in both the QMB and FMB methods is the use of an exclusive non-overlapping movement authority known as a PTC Exclusive Authority (PTCEA) to grant movement authority to each train in the territory. Moving Block Office (MBO) functions manage the creation of the PTCEA messages which are delivered electronically and are artifacts crews depend on for safe train operation. Therefore, the data within these messages are vital and require validation for the safety of rail network operations.

As a spin-off of the QMB project, this research project was created to develop system engineering documents for an OSC component that validates MBO functions that are considered safety critical.

1.2 Objectives

The objective of this project was to produce supporting system engineering documents for the OSC functionality that each railroad can use to pursue further development. These documents include the following:

- OSC ConOps
- OSC SegRs
- OSC Safety Analysis

1.3 Overall Approach

The project included regular meetings with the project's technical advisory group (TAG) to 1) present the progress of the project, 2) discuss and make decisions about project-related issues, 3) discuss the concepts of the proposed OSC component, and 4) present and review results of technical analyses. The work was conducted with a combination of the following tasks:

- The development of an OSC ConOps, including architecture, features, functions, failure modes, and a high-level implementation plan.

- The development of functional and non-functional requirements for the OSC component.
- The development of the initial OSC safety analyses, including a preliminary hazard analysis (PHA), a system hazard analysis (SHA), and an operation and support hazard analysis (O&SHA).

1.4 Scope

The proposed OSC is a component of a Moving Block train control system that provides validation for safety-critical MBO functions. The OSC specification also encompasses the functionality needed to satisfy the PTC Back Office Server (BOS) functions that require safety-critical validation when used for QMB or FMB operations, i.e., OSC functions that are not limited to checking MBO functionality. This extended validation relates to PTC-BOS functions that process safety-critical information exchanged between the Office and the O-PTC, QMB, and FMB trains (e.g., track bulletins) that have already been defined in Standard S-9361 [3] as those that require Redundant Integrity Check Cyclic Redundant Check (RIC CRC).

The system engineering documents produced as part of this project are not intended to duplicate requirements already addressed by QMB or other Interoperable Train Control (ITC) specifications. Rather, the documents specify the requirements for OSC to validate safety-critical MBO and PTC-BOS functions.

Centralized Interlocking (CIXL) is an optional QMB implementation component, and its system requirements have yet to be developed, therefore, this component will not be addressed in this project. The OSC documentation produced during this project will have to be updated if/when CIXL functions that require OSC safety-critical validation are fully developed.

The OSC safety analyses provide the hazard descriptions, mitigations, and risk assessment results from the analysis of QMB and O-PTC operating with OSC support. The analyses were limited to the hazards related to the MBO functions that require a higher safety integrity level in QMB, as compared with the safety level necessary for O-PTC, to the extent that safety and hazard mitigation information is available on the current O-PTC system. The safety analyses are also limited to O-PTC risks that can be mitigated with OSC functions.

1.5 Organization of the Report

The report is divided into the following sections:

- Section 1 provides background information on the project to aid in setting the context for the work performed.
- Section 2 provides an overview of the OSC project tasks and deliverables.
- Section 3 contains the conclusions of the project and recommendations for next steps.
- Appendix A contains the OSC ConOps.
- Appendix B contains the OSC SegRs.
- Appendix C contains the OSC Safety Analyses.

2. Project Overview

The project consisted of the following tasks that, when combined, establish the foundation for the proposed OSC component:

- ConOps
- SegRs
- Safety Analyses

Each of these tasks resulted in standalone documents included as appendices to this report.

2.1 OSC ConOps

From a functional standpoint, the OSC validates the group of MBO and PTC-BOS functions considered to be safety-critical. Complete office functionality is performed in the MBO and the PTC-BOS. While the OSC does not introduce operational functionality beyond what is provided by the MBO and PTC-BOS systems, it is designed to satisfy the safety requirements and system design characteristics that must be pursued to allow those functions to be implemented in a fail-safe manner.

Appendix C of CFR49 Part 236 [1] states that product design must include the Safety Assurance Concepts (SAC) described in standard IEEE 1483-2000 [2] to ensure 1) that failures will be detected and 2) that the product will automatically be placed in a safe state when failures occur. The team adopted the Diversity and Self-Checking SAC defined in IEEE1483-2000 and in Appendix C of 49CFR236 Subpart I as the SAC for the OSC because this SAC accommodates the use of a safety checker. The proposed OSC architecture is advantageous from the perspective that it will accomplish the following:

- It will reduce the vitality of minimum functions. When used in conjunction with a fail-safe onboard segment that verifies CRCs and Hash-based Message Authentication Codes (HMACs) applied by diverse office systems, the proposed OSC architecture can achieve a fail-safe level of safety integrity for vital QMB functions without requiring any individual office component or subsystem to be fail-safe on its own.
- It will contain the entire OSC in a single environment.
- It will decouple the proposed architecture from functions that implement business functions (such as Computer-Aided Dispatch (CAD) Movement Authority (MA) parsing or CAD interface functions) that do not necessarily need a fail-safe implementation. For example, the PTCEA Manager can be designed, implemented, and maintained independently from the OSC.
- It will provide loose coupling with other office components to allow full reuse of a railroad's existing PTC-BOS without requiring the OSC to access any interfaces that are internal to the PTC-BOS. The OSC uses the same inputs and outputs as the PTCEA Manager and PTC-BOS.
- It keeps the OSC functionality as simple as possible.

Although this safety checker architecture is fail-safe, it is not necessarily fault tolerant. It can be made fault tolerant by implementing triple-redundant pairs of PTCEA Managers and OSCs, or by using other possible architectures and/or SACs. Achieving fault tolerance is beyond the scope of this project.

In the proposed architecture, the OSC interfaces with a railroad's CAD system, the PTCEA Manager, and the PTC-BOS components. The OSC needs to have its own copy of the track database and, if the master source of this database resides in a system other than the CAD or the PTC-BOS, the OSC will have to interface with that system.

In the proposed concept, the OSC checks that every safety-critical office function is performed safely. The OSC uses the RIC concept defined in the Interface Control Document (ICD) S-9361 [3] to mark a safety-critical message from the Office as having been validated by the OSC and checkable for errors by the onboard segment receiving the message.

As the OSC validates the results of a safety-critical function, it calculates an RIC CRC and inserts this information in the message that contains the results of the safety-critical function, indicating that message has been safety validated by the Office. The message is then sent back to the PTC-BOS that will send it to the addressed train(s). The train's onboard segment checks to ensure the message contents are consistent with the RIC CRC. This check is similar to the check performed by the PTC-BOS regarding the HMAC and/or CRC applied to the message. If the CRC or HMAC validation checks fail for any of the onboard segments due to the message containing an incorrect or empty RIC CRC or an error during the validation computation, the onboard segment will discard the message and send a notification to the MBO.

The OSC ConOps can be found in Appendix A.

2.2 OSC SegRS

The OSC SegRS defines the functions that the OSC must perform to validate the safety-critical functions of the MBO and the PTC-BOS. The segment-level requirements in this specification focus on railroads' needs and not on implementation solutions to leave the maximum possible flexibility for each railroad and OSC supplier to develop their most effective design.

The OSC SegRS can be found in Appendix B.

2.3 OSC Safety Analyses

The team performed OSC safety analyses limited to the hazards related to the MBO functions that are different in the QMB (including OSC) as compared with Overlay PTC (O-PTC) and also included risks identified in PTC-BOS safety-critical functions that can be mitigated with OSC implementation. These risks were analyzed to the extent possible given the information available in the O-PTC system.

The safety analysis was performed from three standard perspectives culminating in a Hazard Risk Assessment (HRA). The three perspectives are:

- PHA
- SHA
- O&SHA

The safety analyses the team developed during this project are preliminary drafts that will require further updates by any railroad choosing to implement a QMB system (including OSC) to account for railroad-specific characteristics and details of the O-PTC system.

The safety analyses can be found in Appendix C, which provides hazard descriptions, mitigations, and risk assessment results from the analysis of the OSC concept and requirements.

3. Conclusions

The research team worked with the railroad industry and produced system engineering documents for the OSC component. This effort included the development of the ConOps, SegRS, and Safety Analyses. The main conclusions from the effort include the following:

- The proposed OSC does not add operational functionality to the MBO and O-PTC systems. It is designed to satisfy the safety requirements and system design characteristics that enable safety-critical QMB functions to be implemented in a fail-safe manner.
- The QMB/FMB safety-critical functions included in the OSC design are those primarily related to the issuance and validation of PTCEAs.
- The team applied the Diversity and Self-Checking SAC defined in IEEE-1483-2000 [2] and Appendix C of 49CFR236 [1] Subpart I collectively to the PTCEA Manager, the PTC-BOS, and the OSC segments working together with the onboard segment such that each vital office function is performed in two of the three diverse office segments (one of which is always the OSC). Critical components perform internal self-checking.
- OSC functionality works in conjunction with the PTCEA Manager so that the MBO can perform QMB and/or FMB office functions in a fail-safe manner. Therefore, the implementation of the OSC must occur simultaneously with the implementation of the remaining MBO components.
- The OSC safety-checking functionalities related to the PTC-BOS (e.g., track bulletin safety checking, office segment poll, and current dataset list messages) are required, and may be implemented within the OSC or alternatively in a different segment (e.g., at the track bulletin source) based on each railroad's needs (some railroads may have other means to perform safety checking functionalities).
- The OSC safety analyses include the identification of potential hazards associated with the MBO and PTC-BOS safety-critical functions, the risks associated with these hazards, and how these risks can be eliminated or mitigated. These analyses conclude that the risks can be mitigated to an acceptable level with OSC implementation.
- The safety analyses performed in this project are preliminary drafts that will require further updates by any railroad choosing to implement the QMB system (including OSC) to account for railroad-specific characteristics.

4. References

[1] U.S. Government Publishing Office, Title 49 Code of Federal Regulations Part 236, Appendix C to Part 236– Safety Assurance Criteria and Processes, Washington, DC: Federal Railroad Administration.

[2] Report: Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control," IEEE, 2000.

[3] Association of American Railroads, "PTC Office-Locomotive Segment - ICD Standard S-9361 V2.0," *Manual of Standards and Recommended Practices*, Washington, DC: AAR, 2014.

Appendix A. Concept of Operations

Operational Concept Document

for the

Moving Block Train Control Office Safety Checker (OSC)

Prepared by

Transportation Technology Center, Inc.

Version 2.0

November 22nd, 2021

The information in this document is based upon work supported by the Federal Railroad Administration under contract DTFR5311-D00008L. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the author(s) and do not necessarily reflect the views of FRA or U.S. Department of Transportation.

REVISION RECORD

VER	DESCRIPTION OF CHANGE	DATE
1.3	Draft Release	6/28/2021
2.0	Updated for final report	11/22/2021

1 Introduction

New methods of train control that have the potential to enhance safety, reliability, and operational performance have been identified and researched as part of an ongoing program to support higher reliability and capacity train control (HRCTC). The new methods build upon the existing Positive Train Control (PTC) system in the form of additional modes of operation for use in designated territories.

The HRCTC program addresses Enhanced Overlay PTC (EO-PTC), Quasi-Moving Block (QMB), and Full-Moving Block (FMB) methods of train control. In the implementation of both QMB and FMB, a movement authority known as a PTC Exclusive Authority (PTCEA) is provided to each train in the form of "From" and "To" limits that can be assigned to any track location, not necessarily confined to fixed (block) locations. PTCEAs are dynamically updated automatically by MBO functions in a moving block manner as trains move along the track. In a QMB operation, track circuits are used for broken rail detection.

In QMB, PTCEAs are issued by the PTCEA Manager for every train operation. This procedure offers safety improvements over current Overlay PTC (O-PTC), including the ability to provide restricted speed collision protection, such as rear-end collision protection and, in certain configurations, collision protection within a joint authority for trains operating under exclusive authority. Certain implementations of QMB also provide a portion of the traffic capacity benefit of FMB.

Taking advantage of the PTCEA concept, Centralized Interlocking (CIXL), a spin-off of QMB, is focused on the option to eliminate core interlocking functions of current signaling systems with the addition of Office functions to perform the functions eliminated in the field and vital command wayside devices.

Both the QMB and CIXL systems require the implementation of a group of safety-critical functions in the Office. While these functions are or will be included in the PTCEA Manager and the PTC-BOS to make them fail-safe, an Office Safety Checker (OSC) can be used to provide an independent real-time check to ensure these functions are performed correctly. The OSC functions may be implemented in an independent stand-alone server or may be integrated with PTCEA Manager and PTC-BOS hosts. This document presents the OSC concept of operations (ConOps) as a stand-alone functionality. CIXL is an optional QMB implementation component, and the safety-critical functions of CIXL and QMB are differentiated as such in this document.

1.1 Purpose

The purpose of this document is to describe the operational concepts of an OSC. New concepts that leverage QMB and CIXL concepts are proposed as well.

1.2 Scope

The scope of this document includes the following:

- A description of conceptual functions
- Key design details

- Configurations
- Dependencies
- Operator interactions
- Interfaces with the OSC
- A high-level system architecture
- A high-level implementation plan

The analysis included in this document was based on the group of safety-critical functionalities required for the implementation of QMB and CIXL. The OSC can also check safety-critical functions required for the implementation of the FMB Office component when those functions are fully defined/implemented. It is assumed that FMB implementation, if such happens, will only require limited expansion of the OSC functional capabilities but no new technology.

1.3 Document Overview

- Section 1 presents general information about the document.
- Section 2 is an overview of current and planned train control systems, both QMB with field interlocking and QMB with CIXL.
- Section 3 summarizes the benefits of QMB and CIXL.
- Section 4 describes the core principles and architecture of the OSC and presents its operational concepts.
- Section 5 discuss the operational scenarios under OSC.
- Section 6 presents preliminary assessment of failure modes and responses.
- Appendix A-1 includes a description of safety-critical functionalities for the CIXL system.

2 Current System

2.1 Conventional Train Control

2.1.1 CTC Territory

One of the conventional modern types of signaled territory for higher density lines is Centralized Traffic Control (CTC). A typical CTC installation allows a dispatcher to manage traffic remotely via field interlocking (IXL) systems and the associated wayside signals. Signals in CTC territory, except for automatic interlockings at diamonds, fit one of two types: 1) control point (CP), an absolute signal that is remotely controlled by a train dispatcher, or 2) an intermediate signal, a signal that is controlled automatically by the conditions of the track in that signal's block and by the condition of the signal ahead. CPs designate the boundaries of control blocks for interlocking and are located at the extremities of sidings, junctions, crossovers between adjacent tracks, and manual diamond crossings. Codeline systems are used to link the Computer-Aided Dispatch (CAD) system with the field IXL. The dispatcher requests a route, the request is sent to field IXL logic at CPs along the route via the codeline system, and safety is verified in a fail-safe manner by the field IXL before execution.

Figure 1 provides an illustration of a typical CTC with single and multiple tracks. As shown, a control block spans the gap between two CPs. Typically, multiple intermediate blocks are located within a control block and employ Automatic Block Signaling (ABS). The ABS system relies on track circuits for track occupancy and broken rail detection. Information about the status of each block is typically transmitted to adjacent blocks using coded track circuits, and the electrical signal that is transmitted through the rails is coded using different pulse rates to indicate the signal aspect that block is currently displaying. This information is interpreted by the equipment at the adjacent block limit and used in determining the proper aspect to display for the signal governing movement over that block.

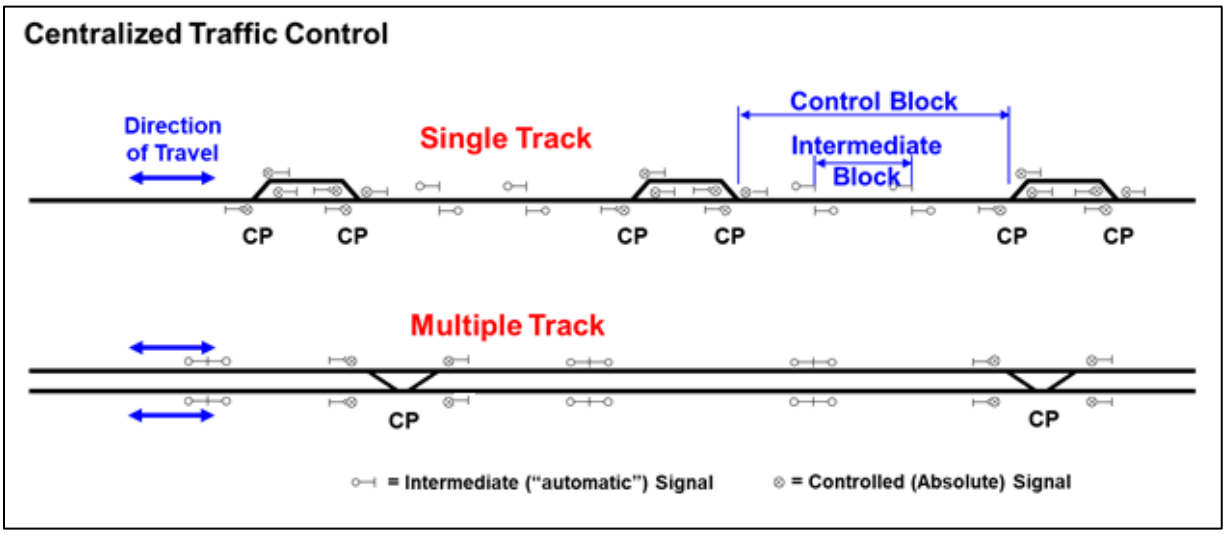


Figure 1. Schematic of Typical CTC Territory

2.1.2 Non-CTC Territory

In non-signaled territory, the dispatcher issues authority for a specific train to occupy a given section of track. Track Warrant Control (TWC) is the general code of operating rules (GCOR) method of train control used in non-signaled territory. Other operating rules use methods similar to TWC in non-signaled territory. The QMB operation requires track circuits and is not applicable to non-signaled territory unless track circuits are installed throughout the territory. However, a QMB system includes all functionality necessary to support a Full Moving Block (FMB) operation in non-signaled territory, especially if QMB trains are programmed to disable track circuit-related restrictions when operating in territory identified as non-signaled FMB territory.

It is possible to have a combination of TWC and ABS (TWC-ABS) where the track warrant grants movement authority instead of CPs, and the ABS system provides train separation within track where the track warrants overlap and broken rail protection. TWC-ABS territory is amenable to conversion to QMB operation since track circuits are already present.

2.2 Positive Train Control

The Rail Safety Improvement Act of 2008 (RSIA ’08) mandated the implementation of interoperable PTC on a significant portion of rail lines in the United States. PTC, as defined in the RSIA ’08, is a system designed to prevent train-to-train collisions, overspeed derailments, unauthorized incursions into established roadway work zones, and the movement of a train through a mainline switch in the wrong position. Several systems have been developed and implemented to satisfy the PTC requirements. The most predominant system is defined by the Interoperable Train Control (ITC) standards that were developed by the largest US Class I railroads.

Figure 2 illustrates the high-level architecture of the ITC system. Using a global positioning system (GPS), a tachometer, and an onboard segment track database, the locomotive onboard segment determines the location of the train relative to both the track and critical assets along the track. Consist and route information, among other data, are provided to the locomotive onboard segment from the PTC-BOS during initialization. Work zones, temporary speed restrictions, and other bulletin data is provided to the locomotive onboard segment by the PTC-BOS over the wireless communications network. Wayside Interface Units (WIUs) installed at switch and signal locations along the track periodically broadcast the status of the switch(es) and/or signal(s) they are monitoring over the wireless communications network. As the train approaches these locations, the status messages are received by the locomotive onboard segment.

The operational data provided to the locomotive onboard segment is processed to determine the real-time operational limits (authority and speed restrictions) for that train. The locomotive onboard segment regularly updates the predicted braking distance of the train and warns the train crew if the train is predicted to violate an authority or speed limit. Additionally, the system can enforce the limits with a penalty brake application (should the crew fail to take appropriate action) to prevent the violation.

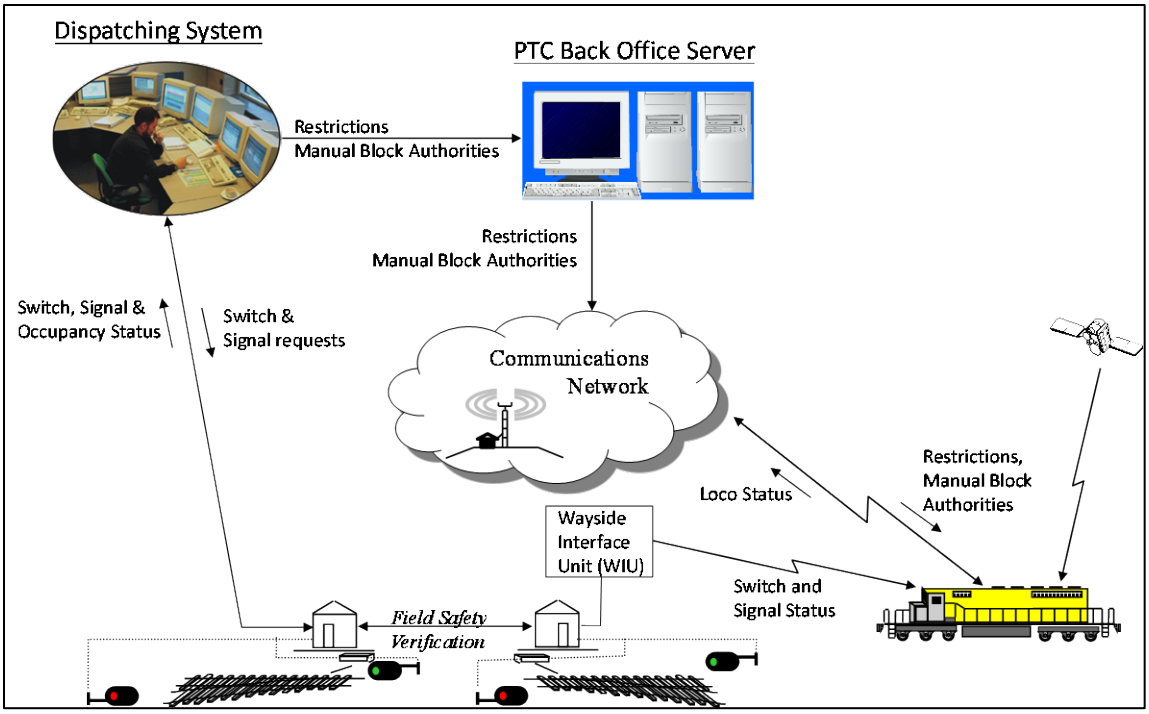


Figure 2. High-level Architecture of ITC (O-PTC) System

2.3 Enhanced Overlay Positive Train Control

In conventional train control, Approach and Advance Approach signal aspects are used to convey conservative speed restrictions to the engineer within blocks governed by these signals. This is done to help the train crew come to a stop within a safe distance of a signal showing a Stop or Restricting aspect. With Enhanced-Overlay PTC (EO-PTC), the operating rules and the onboard segment no longer require or convey speed restrictions associated with Approach and Advance Approach signal aspects because the braking curve generated by the onboard segment enforces the speed at any location within these blocks. These operating rules allow EO-PTC trains to achieve shorter headways while maintaining track speed (Figure 3) by remapping Approach and Advance Approach signals to “Clear” in the track database file used by the onboard PTC segment (Figure 4).

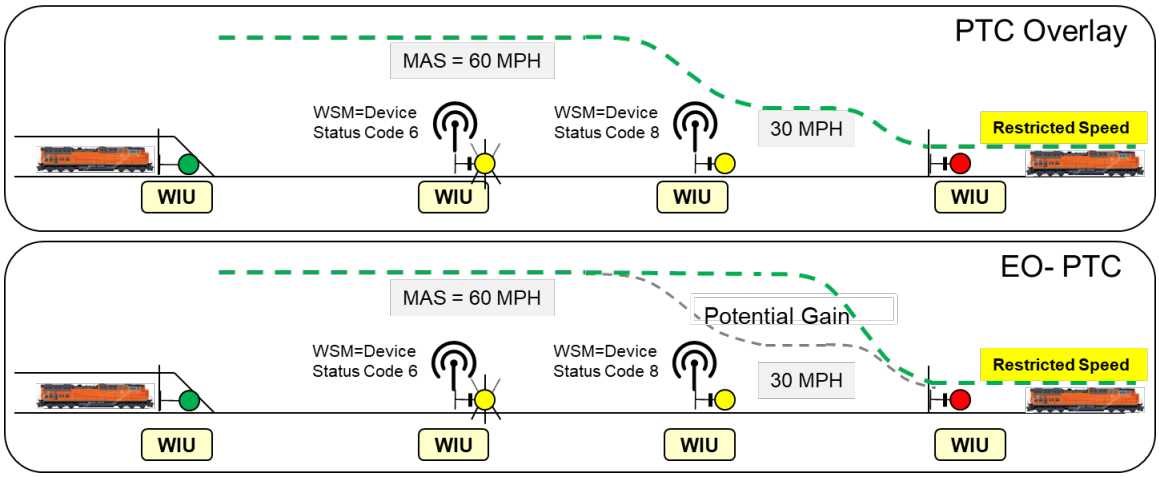


Figure 3. Wayside Signal Aspects and WSMs in Overlay PTC and EO-PTC

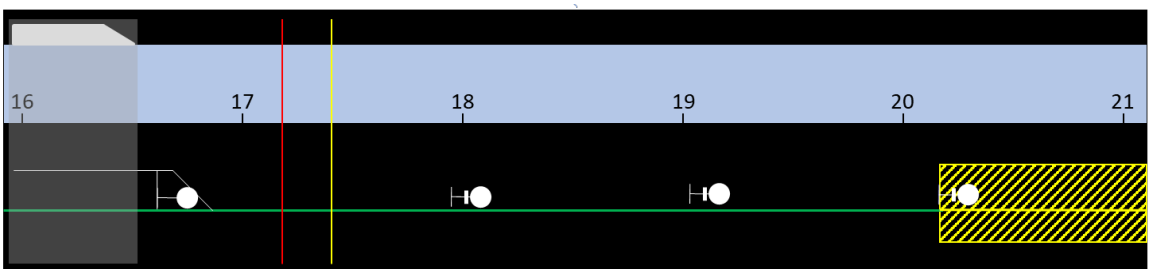


Figure 4. Onboard Display in EO-PTC

Rule changes are required for EO-PTC to account for the discrepancy that would otherwise be caused by the wayside signal and the onboard segment mapping of the signal. For example, the engineer sees a solid yellow aspect displayed on the field signal, but the onboard display shows a green track line. The rules need to allow the engineer to follow the more permissive indication given by the onboard display.

EO-PTC does not alter the movement authority granted by existing train control or signal systems, it only changes the point at which trains must begin decelerating from maximum authorized speed (MAS) in the Approach and Advance Approach blocks. Crews are responsible for being able to stop their trains short of a red signal, as in conventional signaled territory, and short of a "To" limit in non-signaled territory.

2.4 Quasi-Moving Block

Not only does QMB inherit most of the design of the existing Interoperable Train Control PTC (ITC-PTC) architecture, it also inherits the EO-PTC method of handling Approach and Advance Approach signal aspects. Figure 5 illustrates an example of the overall QMB architecture. The onboard segment both retains all the existing core functionality of the O-PTC system and continues to obtain the status of the field devices from Wayside Status Messages (WSMs) generated by WIUs. The PTC-BOS continues to be the interface between the Office and the field. To support QMB, minimal changes to existing CAD systems and functions are needed.

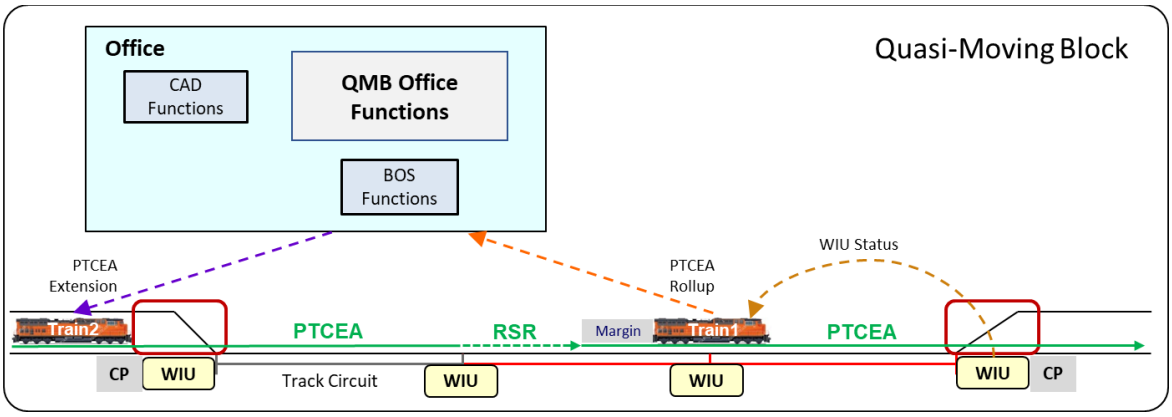


Figure 5. QMB Functional Architecture Diagram

Train movement authorities originate from the CAD system and can overlap. Moving Block Office (MBO) functionality parses any CAD movement authorities (CAD-MAs) that overlap into exclusive PTCEAs. PTCEAs provide the authority for train movements and track occupancy. Based on the most restrictive PTCEAs, WSMs, train-specific speed restrictions (where applicable), and permanent and temporary track speed restrictions, the onboard segment determines speed and authority limit targets.

The onboard segment includes new functions for a QMB operation. One of these new functions is for a QMB train to automatically roll up its own PTCEA. This function involves determining the end-of-train (EOT) location, either with or without a Vital Rear-of-Train Location (VRTL) determination. In basic QMB operations (i.e., without VRTL and with conventional broken rail detection based on track circuits), a following train is allowed to enter an occupied track circuit at Restricted Speed (Figure 5). In advanced QMB implementations, the onboard segment permits entry into an occupied track circuit at MAS under certain conditions. In addition to HMAC or other CRC verifications performed as part of O-PTC functionality, the QMB system also requires the onboard segment to verify the correctness of each safety-critical message received from the Office per the message's Redundant Integrity Check Cyclic Redundant Check (RIC CRC).

QMB introduces a new set of functions for the Office as well. These functions are responsible for the management of all PTCEAs in the system that tracks the following:

- PTCEAs that have been issued
- PTCEAs in which roll-ups/extensions have occurred
- Segments of track reserved with PTCEAs for trains
- Segments of track available for use

2.4.1 QMB with Field Interlocking

Figure 6 illustrates the functional design of QMB implemented with conventional field IXL in CTC territory. The PTCEA Manager is the main component that introduces new functions in the Office with QMB. It is responsible for processing CAD-MAs, validating them. and converting them into PTCEAs, which are then stored and sent to trains through the PTC-BOS components (PTC and Interoperable Train Control Messaging (ITCM)). As currently done with O-PTC, the

commands to the field IXL continue to be sent directly from CAD to the field IXL, illustrated in Figure 6, e.g., using CTC over ITCM communication. The PTC onboard segment processes PTCEAs and verifies the consistency of the route contained within it with the status of field devices (i.e., signals, switches) that are obtained from WSMs, as with O-PTC.

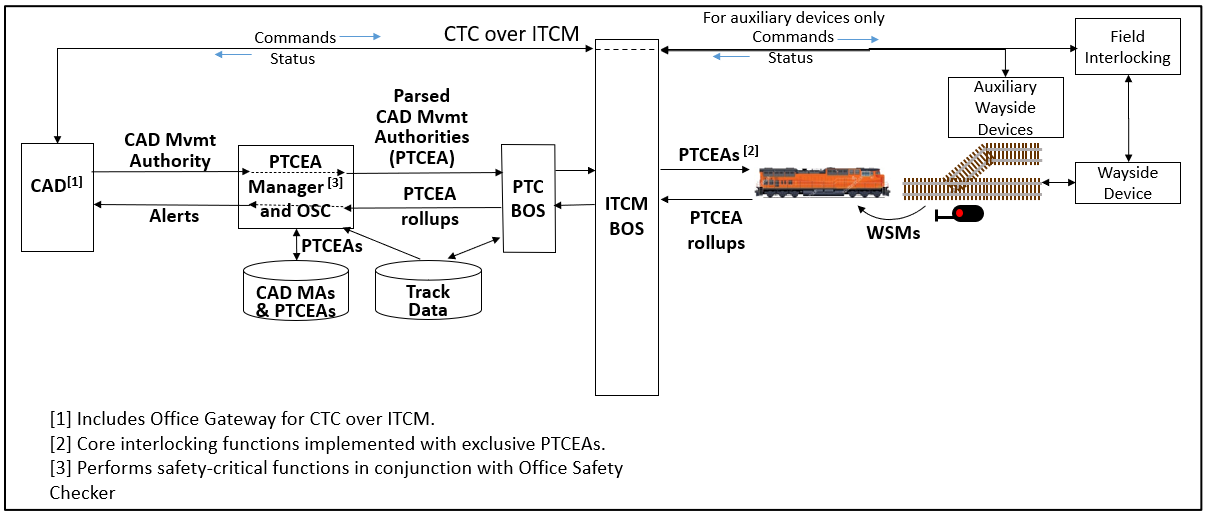


Figure 6. QMB Functional Architecture with Field Interlocking

2.4.2 QMB with Centralized Interlocking

Figure 7 illustrates the functional architecture of QMB with CIXL. The main differences of QMB with CIXL compared to QMB with field IXL include the elimination of core IXL functions from the field and the addition of CIXL functions and components in the Office and in the field.

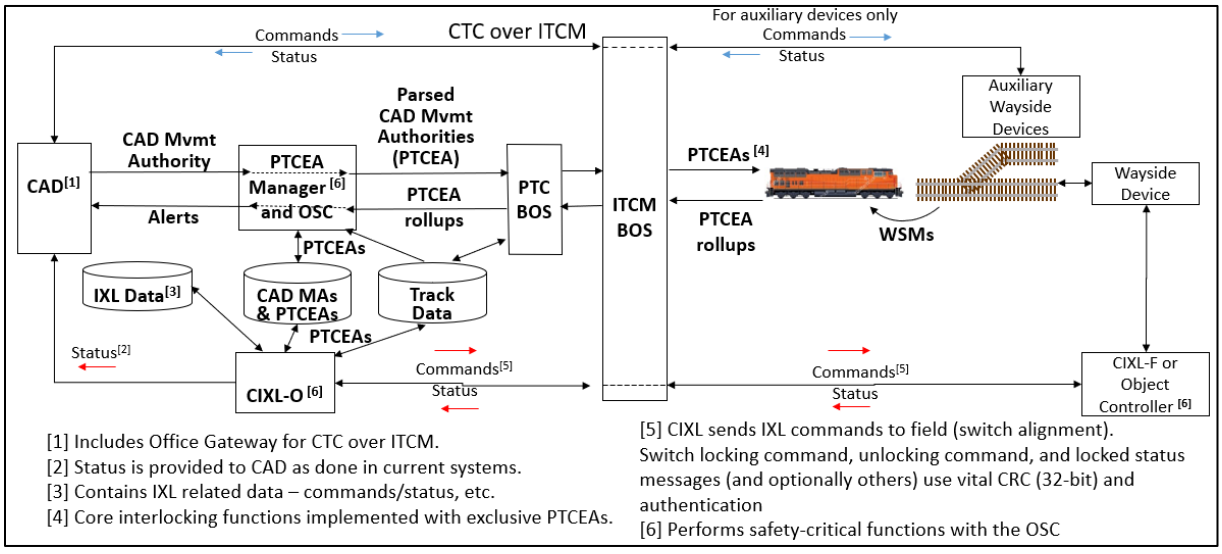


Figure 7. QMB Architecture with CIXL

CIXL introduces two components containing safety-critical functions: 1) the CIXL Office Segment (CIXL-O) and 2) the CIXL Field Segment (CIXL-F) or object controller (OC).

- The CIXL-O performs the interlocking functions in conjunction with the PTCEA Manager and the CIXL-F segment. The primary function of CIXL-O is to convert a train's PTCEA into wayside commands and send them to the CIXL-F of the corresponding CPs. When a train clears the CP and rolls up its PTCEA (except for locations where derails are installed and need to be thrown back to normal to prevent a roll-out from reaching the mainline), CIXL-O does not send a message to each CP commanding it to unlock its field device(s). When the next PTCEA is issued through the CP, CIXL-O sends an unlock command only if the switch position needs to move. Due to rollups and extensions of limits, a train may receive PTCEA updates through the same CP as it approaches and then passes through that CP. To avoid sending unnecessary, redundant messages, CIXL-O only sends one switch position/lock command to an OC when the first of those PTCEAs is issued. Authentication is used on lock and unlock commands to protect against an unauthorized entity changing a train's route. Retransmissions are sent if no acknowledgement is received from CIXL-F. CIXL-O also performs any additional interlocking functions (not already implemented by the PTCEA Manager), receives the field devices' statuses, creates log entries, and forwards the status of wayside devices to CAD. CIXL-O also coordinates the operation of local control functions in the field.
- The CIXL-F or OC is installed at each CP location. The OC receives device (e.g., switch) commands from CIXL-O and controls the wayside devices through direct control connections. The wayside devices include all switches, movable point frogs, On Sheet (O/S) track circuits, and/or any field device that is remotely controlled or whose status is monitored by an OC. The OC monitors the status of the associated wayside device(s) and forwards the status back to CIXL-O whenever the state of the wayside device(s) changes. Heartbeat messages are also sent periodically to confirm the OC health and status of the wayside device(s). The OC also interfaces with any other CP functions that remain in the field if the functions require an interface with the Office. The basic OC functionality steps include translating a) command messages received over the PTC network from CIXL-O into binary discrete device control signals and b) binary discrete status from wayside devices into status messages to send to CIXL-O. The OC may optionally perform other local functions that do not benefit from centralization, e.g., occupancy locking of switches per their O/S circuits. It is important to note that some or all of the current CP hardware may be reused to implement the OC hardware, and in that case, it only has to be re-programmed/re-configured to implement the required CIXL field functions.

3 Justification for OSC

The OSC performs a set of core safety-critical function checks for the implementation of QMB and CIXL systems. Since these systems must safely accommodate standalone train control operation, they contain functions that must be implemented in a fail-safe design. While OSC does not introduce *operational* functionality to QMB and CIXL systems, it is designed to satisfy the safety requirements and system design characteristics that allow those functions to be implemented in a fail-safe manner.

QMB is part of a strategic plan to provide higher reliability and capacity train control. QMB can provide benefits in reliability, safety, and capacity as seen in Table 1. These benefits come at the cost of adding new Office functions and additional functions for the onboard segment. Although it allows the elimination of physical signals, basic QMB does not require any modifications to the wayside. Optional technologies, including VRTL and advanced track circuits, bring further benefits.

Table 1. QMB Expected Benefits

Category	Expected Benefit
Safety	Collision protection at all speeds (including restricted speeds); vital when using VRTL determination
	Pull-apart protection applies in any event when VRTL reports indicate a greater train length than estimated, where the pulled-apart cars are protected by a PTCEA
	Improved loss-of-shunt protection (using movement authorities, train location reports, and train length data as additional sources of occupancy detection)
	Uniform method of train control (whether CTC, ABS, or dark territory) using PTCEAs
	Verification that crew track selection matches authorized tracks included in train's movement authority (Note: may already be done to some extent in PTC implementations)
Capacity & Efficiency	Increased capacity beyond that of EO-PTC if track circuits are shortened, more feasible with QMB, due to the elimination of wayside signals (and therefore no need for additional aspects), reduced wayside logic, possible use of jointless track circuits, and/or possible use of ≥1,000 MGT insulated joints.
	Increased capacity beyond that of EO-PTC using advanced broken rail detection within an occupied block (e.g., next generation track circuits[1]), along with VRTL[2]. A following train may enter an occupied intermediate track circuit at MAS and maintain MAS per the braking curve. This achieves the same reduction in headways and increases in traffic capacity as FMB train control when a following train's braking distance is greater than one track circuit block length.
	QMB can reduce delays caused by approach and time locking. When a dispatcher needs to change a route already assigned to a train and the train's braking curve indicates the train can stop before the CP or interlocking, the route can be changed without time penalty.
Reliability-Maintainability	Facilitates removal of signal heads and simplifies some vital field logic, such as coded track circuits.
	QMB with CIXL simplifies and reduces field components (such as field logic devices, cabling, etc.) and facilitates diagnostics and maintenance.

[1] J. Kindt, J. Brosseau, and A. Polivka, "Next Generation Track Circuits," Federal Railroad Administration, 2018.

[2] Alternate means to achieve capacity benefit (without requiring VRTL) is to deploy track circuits that detect specific location of a train or rail break within a block.

4 Concepts for the Proposed System

Based on the principles and the functional description of the QMB and CIXL Office functions that are considered safety-critical, this section introduces potential functional architectures that can be pursued for fail-safe implementation. OSC functionality is applicable to both FMB and QMB. The OSC should also be capable of hosting any additional safety-critical functionality that may be required for the implementation of FMB, if that becomes necessary. It is assumed that if and when FMB is implemented, it will require the limited expansion of software functionality but no new technology or change in a chosen architectural design for OSC.

4.1 QMB Core Principles

The QMB method of train control is based on several core principles:

- Train authority is granted by exclusive PTCEAs – non-overlapping and electronically delivered movement authorities.
    - Every train or other rail vehicle must have a PTCEA to enter and occupy controlled mainline track, even non-enforcing, non-communicating (NENC) trains.
    - Management of PTCEAs is centralized in the Office, including responsibility for extending PTCEAs (although distributed implementation is also possible).
    - Trains are responsible for automatically initiating rollup of their own PTCEAs. (Note: In failure scenarios, the crew verbally communicates with the dispatcher to roll up a PTCEA.)
- PTCEAs are not validated in the Office against the state of field devices for any safety purposes – that is left to the onboard segment that applies the most restrictive of its PTCEAs and absolute WSMs at O/S. This alleviates the need for quick and extremely reliable communication of WSMs from WIUs to the Office.
- The onboard segment determines and enforces speed restrictions, based on the most restrictive PTCEA speed limit (e.g., in the case of a bi-directional authority), train-specific speed restrictions (where applicable), and track speed restrictions (permanent and temporary).
- Use of WIU-to-locomotive peer-to-peer communication, as in O-PTC
- Removal of wayside signals as a part of a migration/implementation plan
- Since QMB is a standalone train control system a crew must rely on for safe operation of the train, one or more safety assurance concepts (SAC) must be applied to vital functions.

Details of the QMB design can be found in the QMB Train Control project report [4].

4.2 CIXL Core Principles

If CIXL is implemented in addition to QMB, many safety-critical functions currently implemented in a distributed manner with field equipment may be centralized, allowing for lifecycle cost savings.

CIXL is based on the following core principles:

- PTCEAs are used as the unique train movement authorization. In QMB, all PTCEAs are exclusive (non-overlapping) and handled in a fail-safe manner.
- Signal indications are eliminated from the interlocking logic and consequently the wayside signals are removed. WSMs transmit the status of both the track circuits (occupied/rail break or clear) and the switches. The elimination of wayside signals may occur prior to, during, or after the implementation of QMB or CIXL.
- The core interlocking functions, i.e., the prevention of conflicting routes among trains, are performed by PTCEAs.
- WSMs convey the status of field devices at CPs directly to trains so that the Office does not require high-rate vital communications with the field.
- The non-overlapping nature of the PTCEAs together with the onboard computer monitoring the field devices in the train route satisfy the safety principles and/or replace interlocking functions such as route and traffic locking.

4.3 OSC Safety Assurance and Verification Concepts

To evaluate the validity of safety objectives, the development of PTC system components must follow the criteria and processes defined in Appendix C to Part 236 of 49 Code of Federal Regulations [1]. The system must be designed to ensure safe operation with no hazardous events under normal anticipated operating conditions with proper inputs and within the expected range of environmental conditions. All safety-critical functions must be performed properly under normal conditions. The system must operate safely even in the absence of prescribed operator actions or procedures.

Appendix C of CFR49 Part 236 states that the product design must include the SAC described in the IEEE-1483 standard [2] to ensure failures are detected, and the product is automatically placed in a safe state when they occur. The IEEE-1483 standard defines a method for the identification and subsequent verification of safety-critical functions implemented in processor-based equipment used in safety-critical applications on rail and transit systems. This standard requires the production of analyses and other supporting documentation to demonstrate the achievement of the established safety goals.

The activities associated with safety verification, as defined in the IEEE-1483 standard, are divided into Conceptual, Functional, and Implementation levels. Concept-level activities 1) analyze the safety assurance concept employed, 2) identify the concept-specific design requirements necessary for the fail-safe implementation of safety-critical functions, and 3) identify the concept-specific verification methods. Functional-level activities identify all user-specified system functions required to be implemented in a fail-safe manner. Implementation-level activities must apply the verification methods determined at the concept level to the implemented system to ensure that the identified set of safety-critical functions has been implemented in a fail-safe manner.

4.3.1 Fail-safe Implementation of Safety-Critical Functions

The SAC principles defined in Appendix C of 49CFR236, related to the IEEE-1483 standard, are as follows:

- **Diversity and self-checking concept:** This concept requires all safety-critical functions to be performed in diverse ways, using diverse software operations and/or diverse hardware channels, and that critical hardware be tested with self-checking routines. Permissive outputs are allowed only if the results of the diverse operations correspond and the self-checking process reveals no failures in either execution of software or in any monitored input or output hardware. If the diverse operations do not agree or if checking reveals critical failures, safety-critical functions and outputs must default to a known safe state.
- **Checked Redundancy concept:** The Checked Redundancy concept requires the implementation of two or more identical, independent hardware units, each executing identical software and performing identical functions. A means is to be provided for the periodic comparison of vital parameters and the results of the independent redundant units, requiring agreement of all compared parameters to assert or maintain a permissive output. If the units do not agree, safety-critical functions and outputs must default to a known safe state.
- **N-version Programming concept:** This concept requires a processor-based product to use at least two software programs to perform identical functions and execute concurrently in a cycle. The software programs must be written by independent teams using different tools. The multiple independently written software programs comprise a redundant system and may be executed either on separate hardware units (which may or may not be identical) or within one hardware unit. A means is to be provided for the comparison of the results and the output states of the multiple redundant software systems. If the system results do not agree, the safety-critical functions and outputs must default to a known safe state.
- **Numerical assurance concept:** This concept requires the state of each vital parameter of the product or system be uniquely represented by a large encoded numerical value, such that permissive results are calculated by pseudo-randomly combining the representative numerical values of each of the critical constituent parameters of a permissive decision. Vital algorithms must be entirely represented by data structures containing numerical values with verified characteristics, and no vital decisions are to be made in the executing software, only by the numerical representations themselves. In the event of critical failures, the safety-critical functions and outputs must default to a known safe state.
- **Intrinsic fail-safe design concept:** Intrinsically fail-safe hardware circuits or systems are those that employ discrete mechanical and/or electrical components. The fail-safe operation of a product or subsystem designed using this principle requires that the effect of every relevant failure mode of each component, and relevant combinations of component failure modes, be considered, analyzed, and documented. This process is typically performed by a comprehensive Failure Modes and Effects Analysis (FMEA) that must show no residual unmitigated failures. In the event of critical failures, the safety-critical functions and outputs must default to a known safe state.

Note that the SAC principles do not dictate how a specific system should be implemented, but the design of the system must be such that the principles are satisfied.

4.4 OSC Functional and Architectural Design

From a functional standpoint, the OSC validates the group of QMB, CIXL, and PTC-BOS Office functions that are safety-critical. Complete QMB Office functionality is performed collectively by the PTCEA Manager, the optional CIXL, and the PTC-BOS – these components create safety-critical messages to send to trains. The OSC does not create messages, rather it checks that every safety-critical Office function is performed correctly by the other Office components, particularly by validating each safety-critical message produced before the message is sent to a train. The PTCEA Manager essentially handles PTCEA-related functions, the CIXL handles interlocking-related functions, and the PTC-BOS handles track bulletin data, track data, and message exchanges between trains and the Office.

Figure 8 illustrates the high-level OSC functional architecture for the two different potential QMB implementations, i.e., QMB with field interlocking and QMB with CIXL.

The following relevant aspects in Figure 8 are highlighted:

- Only one of the interlocking solutions (i.e., centralized or field) is active at a given location, but a railroad may choose which one to implement in each territory, depending on its own assessment of operational needs.
- OSC functions interface only with functional components in the Office (PTCEA Manager, PTC-BOS, and CIXL, if present). OSC functions interface with the onboard and wayside (when CIXL is implemented) safety-critical functions through the PTC-BOS and the radio network, protecting vital information in messages with 32-bit CRCs or HMACs.
- The other Office functional components (PTCEA Manager, PTC-BOS, and CIXL) interface directly among themselves for non-safety-critical functions that require it. These interfaces are considered non-vital.

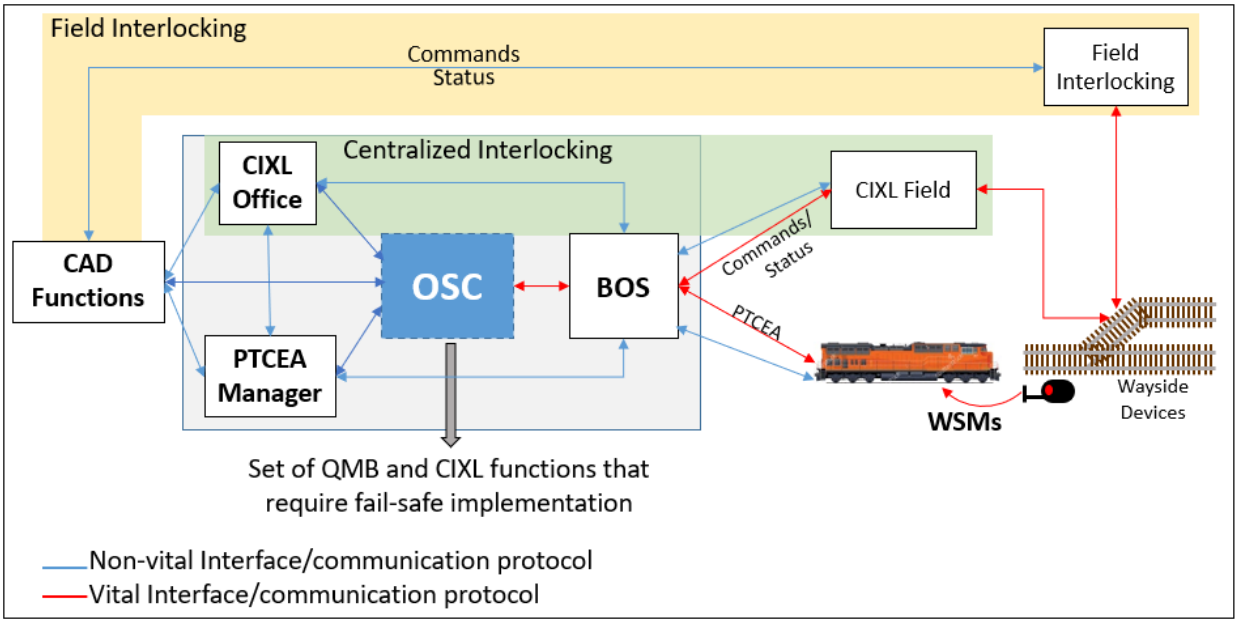


Figure 8. OSC High-Level Functional Architecture Diagram Showing Two Different Interlocking Approaches

The main conceptual element of the interface between the PTCEA Manager functions and the OSC functions is the PTCEA. When a train movement is planned in the CAD system, the CAD sends a CAD-MA request to the PTCEA Manager that converts it to a PTCEA. The PTCEA created by the PTCEA Manager is validated by the OSC and forwarded to the train through the PTC-BOS. Subsequently, when the train has traversed and cleared a portion of the route authorized in its PTCEA, it sends a PTCEA rollup message to the PTC-BOS, which forwards this message to the PTCEA Manager for processing (revising its local copy of the PTCEA to reflect the rolled-up limits), and the results are also validated and similarly processed by the OSC.

The main conceptual element of the interface between the CIXL-O and the OSC is a field command (i.e., switch command). A PTCEA that has been validated by the OSC is also converted to a switch command by CIXL-O. Once validated, the OSC sends the command to the PTC-BOS, which sends it to CIXL-F for execution. Conversely, the status of wayside devices is sent back to PTC-BOS, which forwards it to CIXL for processing.

The OSC also verifies the correctness of the results produced by the PTC-BOS on functions that are considered safety critical before sending those functions to trains. The OSC's verification of whether a Track Bulletin message has been correctly processed by the PTC-BOS includes:

- Converting data from original subdivision/milepost format to PTC block format
- Associating Train IDs to their Locomotive IDs in every Track Bulletin message sent from the Office to trains
- Converting original track bulletin format (e.g., Extensible Markup Language (XML)) to Edge Message Protocol (EMP) format and inclusion of EMP header

The OSC must record the log of activities and persistently maintain the status of all PTCEAs, wayside devices (if CIXL is implemented), track bulletins, and any other safety-critical information. All data must be protected by CRCs.

When the OSC validates the results of a safety-critical function and a message containing these results is to be sent to a train, the OSC generates a RIC CRC and includes this information in the message, indicating the function and message have been safely validated by the OSC. The message is then sent back to the PTC-BOS, which sends it to the addressed train(s). The train's onboard segment checks to see that the message contents are consistent with the RIC CRC in that message, similar to what is done with the HMAC and/or CRC applied to the message by the PTC-BOS. If any of the onboard segment's CRC or HMAC validation checks fail, e.g., due to the message containing an incorrect or empty RIC CRC or due to an error from the validation computation, the onboard segment discards the message and notifies the MBO. There is no need for a RIC CRC to be included in messages received by the Office from a locomotive because the onboard segment is assumed to be fail-safe.

The architecture already implemented by a railroad for its ITC PTC system should be fully reusable and can serve as the foundation for the addition of OSC safety-critical functions if the SAC principles of Diversity and Self Checking defined in Section 4.7.1 are satisfied. A separate server (i.e., independent of the current O-PTC servers), or a mix of existing and new servers, can be chosen for implementing the OSC. Any one of the following options can be adopted:

1. OSC functions hosted on a separate server (Baseline): OSC safety-critical functions are implemented in a hardware and software environment that is separate and diverse from the PTCEA Manager and PTC-BOS. The comparator function required for this SAC is on board each locomotive, in that the onboard segment requires *both* the HMAC and the RIC CRC to be correct before a message is accepted, and these fields were computed and inserted by different, diverse office segments (BOS and OSC). The comparator function is vital and therefore must be implemented in a fail-safe manner. Since the OSC is diverse from other Office segments, it may or may not be designed to be fail-safe on its own, depending on each railroad's safety analysis. Either way, the SAC requirements can be fulfilled to achieve a fail-safe status of vital functions at the system level.
2. An alternative architecture could have the comparator function implemented in the Office, in which case the RIC CRC field would not need to be used for OSC functionality. In this case, the comparator, not the PTC-BOS, could compute and insert the HMAC in messages that it has validated. In any event, the comparator function must have a fail-safe implementation.

Figure 9 illustrates the proposed QMB Office architecture.

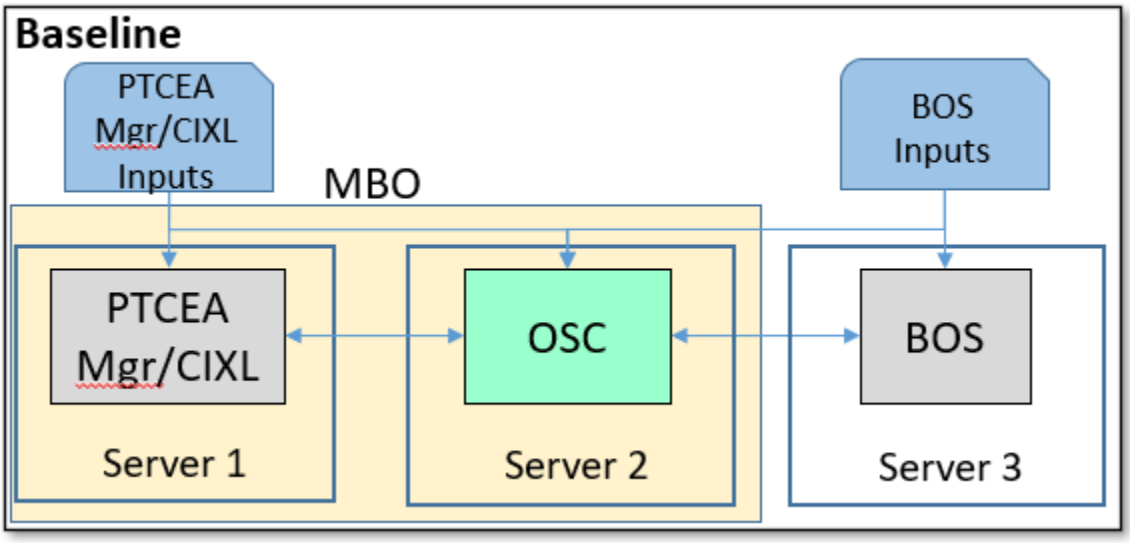


Figure 9. OSC Architectural Design with Diversity and Self-Checking SAC Principle

The following sequence of events based on a CAD-MA request from the CAD system illustrates the principle of the proposed OSC architecture:

- The CAD system sends a train's CAD-MA request to the MBO. Both the PTCEA Manager and OSC receive it.
- The PTCEA Manager validates the CAD-MA and creates a PTCEA for the train, truncating the limits, if necessary, to avoid overlap with another train's PTCEA.
- The PTCEA Manager sends the PTCEA to the PTC-BOS.
- The PTC-BOS processes the PTCEA, converts the limits from subdivision/milepost format to block format, associates to the locomotive ID with the Train ID, and adds the EMP header with HMAC.

- The PTC-BOS sends the PTCEA in EMP format to the OSC.
- The OSC verifies whether the PTCEA is consistent with the original CAD-MA and checks for overlapping PTCEAs in its database and PTC-BOS conversion:
    - If OK, the OSC validates the conversion of the limits from subdivision/milepost format to Block/Offset format, creates an RIC code for the PTCEA, stores it in the OSC database for that train, and sends it to the PTC-BOS.
    - If not OK, the OSC issues an exception to both the CAD system and the PTC-BOS.

From the other direction, i.e., when a train rolls up its PTCEA, the following takes place:

- The PTC-BOS receives a train's PTCEA rollup and forwards it to both the PTCEA Manager and the OSC.
- The PTCEA Manager processes the train's PTCEA rollup (including validating the error check code for the PTCEA with the rolled up "From" limit) and stores the PTCEA update for that train. If there is a following train, the PTCEA Manager can then extend its PTCEA, invoking the process described above.
- The PTCEA Manager sends the PTCEA update to the OSC.
- The OSC compares the following train's PTCEA update sent by the PTCEA Manager with the leading train's PTCEA rollup and checks for overlapping PTCEAs in its database:
    - If OK, the OSC applies the RIC CRC and provides the message to the PTC-BOS for transmission to the following train.
    - If not OK, the OSC issues an exception to both the CAD system and the PTCEA Manager.

It should be noted that the "logic" of the PTCEA Manager and OSC cannot be the same in order to satisfy the Diversity and Self-Checking SAC requirements – the PTCEA Manager implements the functions to parse CAD-MAs into PTCEAs and updates the following train's PTCEAs based on the leading train PTCEA rollups (and other rules), while the OSC just checks the validity of the results from the PTCEA Manager. The OSC uses different (diverse) algorithms from the PTCEA Manager (e.g., for detecting PTCEA overlaps) to avoid common failure modes.

In the proposed architecture (assuming that Diversity and Self-Checking is employed as the SAC), if a function regarding PTCEA creation changes and this change requires only modification to PTCEA Manager source code (not to OSC functions), such modification can be done without requiring vital recertification. This design creates an attractive characteristic for this architecture, i.e., if there is an expectation that algorithms for CAD-MA and PTCEA management may change over time and may differ among railroads. The OSC functions, on the other hand, are only for the purpose of preventing unsafe actions by the MBO (i.e., for enforcing key universal operating rules, not for creating authorities or bulletins), and therefore, are much simpler than the algorithms implemented in the PTCEA Manager and PTC-BOS. Consequently, OSC functionality can be the same for all railroads, as it does not affect proprietary, railroad-specific traffic management functionality.

4.4.1 Alternative Architectures Considered

Figure 10 illustrates the architecture of an alternative QMB office architecture that uses N-version Programming instead of Diversity and Self-Checking SAC. In this alternative, the safety-critical functions are implemented both in each Office component originally responsible for the function (i.e., PTCEA Manager, CIXL, and PTC-BOS) and fully redundantly in one or more OSCs. Therefore, the OSC would be more than a simple "checker," and a different name than OSC would be more appropriate. Distinct hardware and software implementation must be used, and the software programs must be developed by independent design teams, per the N-version Programming SAC. All the inputs received by the PTCEA Manager, CIXL, and PTC-BOS that are required to perform safety-critical functions are also received by the OSC. A separate component, the Comparator, compares the results and output states of the redundant software systems. If the system results do not agree, the safety-critical functions and outputs default to a known safe state, e.g., preventing the issuance of a more permissive authority or restriction. At minimum, the Comparator must be implemented to be fail-safe, while all other components may or may not be fail-safe on their own.

The purpose of this ConOps document is to describe a rudimentary safety checker – a "safety net" that simply prevents unsafe actions by the MBO – not a fully redundant implementation of all MBO safety-critical functions. Diversity and Self-Checking is the only SAC that supports such a concept, (i.e., not N-version Programming). The functionality implemented in the OSC would be different than what is described throughout this document if N-version Programming were used. The functionality would merely duplicate PTCEA Manager/CIXL and PTC-BOS ConOps and requirements specifications with the addition of requirements for a vital Comparator and the requirement that the OSC be developed entirely independently of the PTCEA Manager/CIXL and PTC-BOS.

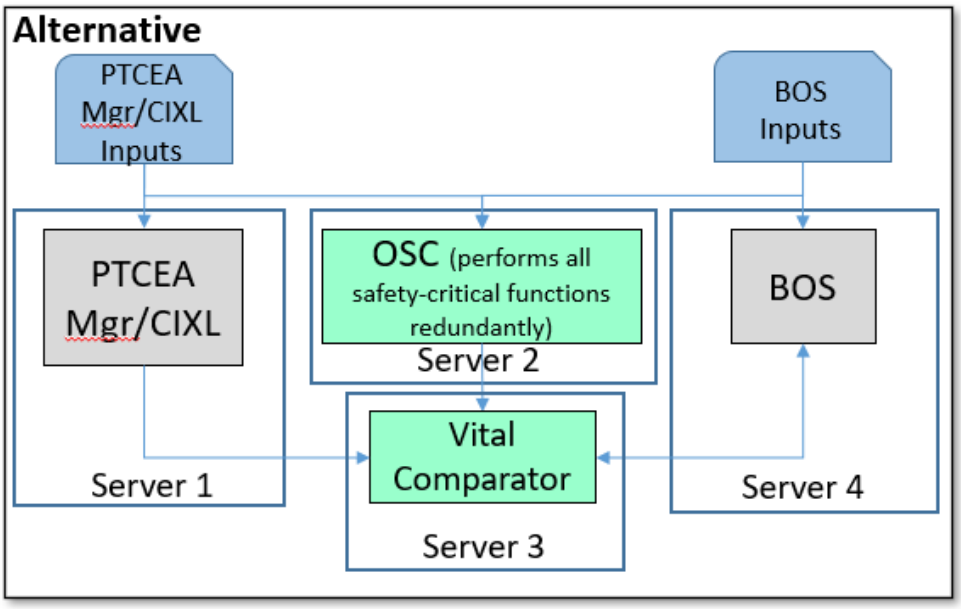


Figure 10. Alternative Architectural Design with N-version Programming SAC Principle

A variant of the N-version Programming architecture (alternative) could be implemented where the Comparator component is in the field (onboard segment and wayside segment, if CIXL is implemented). This variant would eliminate the need for a fail-safe component in the Office.

While theoretically possible, this alternative would require that all outputs of safety-critical functions produced in the Office by the PTC-BOS, PTCEA Manager, and CIXL be sent to the field, requiring a complete redesign of the ICDs and significantly increasing in message traffic loading. Consequently, this architecture is not recommended.

Another alternative could have all MBO functionalities (PTCEA Manager, CIXL, and PTC-BOS) implemented to be fail-safe on their own, not requiring a separate OSC system.

4.4.2 Proposed Architecture Advantages and Functions

The proposed OSC architecture is advantageous from the perspective that it accomplishes the following:

- It reduces the vitality of minimum functions. When used in conjunction with a fail-safe onboard segment that verifies CRCs and HMACs applied by diverse Office systems, the OSC architecture can achieve a fail-safe level of safety integrity for vital QMB functions without requiring any individual Office component or subsystem to be fail-safe on its own.
- It contains the entire OSC in a single environment.
- It decouples from functions that implement business rules (such as CAD-MA parsing or CAD interface functions) that do not necessarily need a fail-safe implementation. The PTCEA Manager can be designed, implemented, and maintained independently from the OSC.
- Based on loose coupling with other Office components, it allows full reuse of a railroad's existing PTC-BOS without requiring the OSC to access any interfaces that are internal to the PTC-BOS. The OSC uses only the same inputs to and outputs from the PTCEA Manager and PTC-BOS.
- It keeps the functionality as simple as possible.

These accomplishments can significantly reduce the need for vital certification when changes to non-safety-critical functions are required.

With the introduction of the OSC, all messages that contain safety-critical information to be sent from the Office to a train's onboard segment must include a RIC CRC that is applied by the OSC in the Office before it is sent to ITCM for transmission to a train. This information includes messages sent from the PTCEA Manager to the onboard segment (e.g., PTCEAs) and from the PTC-BOS to the onboard segment (e.g., track Bulletin Data). In today's O-PTC system implementations, Bulletin Datasets (i.e., 01041 message) and Movement Authority Datasets (i.e., 01051 message) may be sent to a train's onboard segment without the use of a RIC CRC. However, the interface control document S-9361 [3] for Bulletin and Movement Authority Dataset messages already specifies provisions for RIC CRC and defines how it is calculated. For QMB and FMB train control systems using the proposed safety checker architecture, the use of RIC CRCs on vital messages sent from the MBO to a train is mandatory but not optional.

The OSC also verifies the transformation of data types (e.g., XML to EMP) and the association of data (e.g., Train ID to Locomotive ID), in addition to the logical validation of data (e.g., PTCEA limits vs. CAD-MA limits). Details of the validations and calculations performed by the

OSC are provided in Section 5. Figure 11 shows data flows among the different components or segments of the QMB Office.

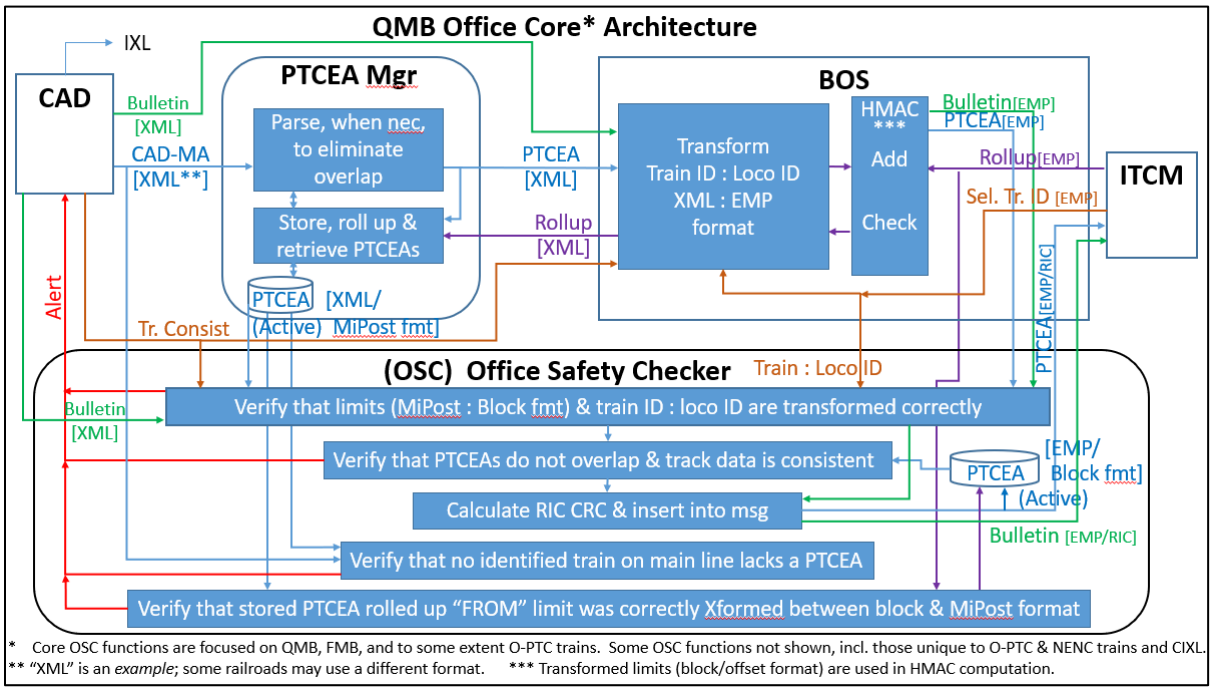


Figure 11. MBO Core Architecture with OSC

Figure 11 also shows how the information is used in the OSC to perform the following basic functions:

- Calculate the RIC CRC and insert it into the specific messages that require it
  - Safety-critical messages sent from the Office to trains require an additional integrity check value (the RIC CRC) that can be verified by the onboard segment to confirm the message validity and the integrity of the information. Since the OSC validates the information of those safety-critical messages, once the information is validated, it calculates and inserts the RIC CRC into the messages before transmitting them using the ITCM. For the case of safety-critical messages that are created in CAD or another non-PTC system and whose user content is not modified by the PTC Office (e.g., track bulletins), the RIC CRC can be calculated and applied at the source (e.g., by the CAD system rather than by the OSC) for better end-to-end protection.
- Verify that PTCEAs do not overlap, and track data is consistent
  - This is the main OSC function. The OSC 1) receives the PTCEAs, 2) verifies that they were created correctly and comply with the non-overlapping requirement, and 3) checks that the PTCEA limits are consistent with the track database. The PTCEAs are sent from the PTCEA Manager to the PTC-BOS in a railroad-specific format (e.g., XML), and the PTC-BOS sends the PTCEA to the OSC as an EMP message. If the PTCEA meets the validation criteria, and the message contains the correct EMP header, the OSC computes and inserts an RIC CRC in the message and sends it back to PTC-BOS which then sends it to the corresponding onboard computer through the

ITCM network. The OSC also checks that the track data in the PTCEA is consistent with the track database.

- Verify PTCEA rollup limits were correctly transformed from block to milepost formats
  - When trains roll up their PTCEA, a new PTCEA is stored in the Office with the rolled up "From" limit. This PTCEA is verified by the OSC to confirm the rollup has been performed correctly. The OSC also checks that the "From" limit has been correctly transformed from Block format to Milepost format.
- Verify that no identified train on the main track in QMB territory lacks a PTCEA
  - The OSC receives information from the CAD system that allows it to validate that every train or other rail vehicle on controlled mainline track in QMB territory has received a PTCEA.
- Validate track bulletins
  - The OSC receives both track bulletin information from the CAD system in a railroad-specific format (e.g., XML) and the bulletin in the EMP message from the PTC-BOS. The information in the message is validated, including the transformation of Train ID to Locomotive ID and track limits from Milepost format to Block format (e.g., in the case of work zone bulletin). The OSC also checks the EMP header of the message, and if correct, calculates and inserts the RIC CRC into the message before sending it back to the PTC-BOS, which sends it to the corresponding onboard computer through the ITCM network. Alternatively, the RIC CRC can be calculated and applied at the source (e.g., by the CAD system) for the case of Track Bulletin messages.

At a minimum, the Comparator must be implemented to be fail-safe, and all the conceptual and functional requirements developed for the OSC remain applicable, whether the rest of the OSC is implemented to be fail-safe on its own.

4.5 OSC System Interfaces

The OSC interfaces with the CAD system, the PTCEA Manager, the PTC-BOS components, and the CIXL (if CIXL is implemented). The OSC does not directly interface with components outside of the Office. The non-vital PTCEA Manager functions include the interface with CAD to receive CAD-MA messages and respond with status and handling of exceptional cases. While in O-PTC territory, CAD-MAs (e.g., track warrants and bidirectional authorities) may be considered safety-critical, whereas in QMB territory, they are merely requests. The PTCEA manager and OSC collectively ensure that movement authorities are safe before issuing them to trains in the form of PTCEAs. The PTCEA Manager may also communicate directly with PTC-BOS components for non-safety-critical functions that require such communication. The PTCEA Manager and the CAD system convey inputs required for safety-critical functions essentially related to PTCEA handling to the OSC. Section 4.5.1 describes the details of such functions.

In a similar fashion, the CIXL functions that are non-safety-critical include the interface with the CAD to report field status and handling of exceptional cases to CAD. The CIXL-O may also need to communicate directly with PTC-BOS components for certain non-safety-critical functions. As the core of vital CIXL functionality resides in the PTCEA creation and validation mechanisms, a few additional CIXL functions are required to be safety critical (Appendix A-1).

4.5.1 Existing Messages and Interfaces

To the extent practicable, OSC interfaces use messages that are already defined for PTC Office components. PTCEA-related messages that are exchanged among PTC-BOS components remain as defined for QMB and CIXL operations.

For the interface between the MBO and the onboard segment, existing ITC messages defined for the conventional PTC system (O-PTC) are used to the extent practicable. Movement authority-related messages, as currently defined for conventional PTC, address most of the needs identified for QMB. A few types of messages have been added or modified to support QMB. The messages containing vital information are validated by OSC safety-critical functions, i.e., when created by the MBO for sending to the PTC-BOS or when received from the PTC-BOS.

For the interface between CIXL and wayside devices, field command and status updates, which may or may not require modification and are defined for CTC over ITCM, can be used. These messages must be created/handled using a vital protocol (e.g., including error checking) by OSC safety-critical functions (as done today with other PTC messages containing vital information) and communicated to the wayside segment through PTC-BOS components.

Existing ITC PTC messages can be found in the AAR Manual of Standards and Recommended Practices (MSRP), Standard S-9361 [3]. Table 2 and Table 3 identify, with some minor modifications, the movement authority-related messages that are used for QMB. These tables do not list other existing ITC PTC messages required for PTC operations that remain unchanged in form and/or function when QMB and OSC are introduced.

Table 2. Movement Authority ITC PTC Messages

Message ID	Message Name
(01051)	Movement Authority Dataset
(02051)	Request Movement Authority
(02052)	Confirmation of Movement Authority
(01053)	Movement Authority Void
(02053)	Confirmation of Movement Authority Void

Table 3. Authority Rollup ITC PTC Messages

Message ID	Message Name
(02050)	Crew Authority Request
(01050)	Confirmation of Crew Authority Request

4.6 OSC Deployment and Migration Path

When QMB and/or CIXL is/are implemented, OSC functionality is also required to assure safety of the vital Office functions of these systems. In other words, the implementation steps of these systems must include the deployment of OSC unless an alternative method of achieving the necessary safety integrity level is used. The most important point to be made about the OSC deployment/migration path is that the verification and validation of OSC functions must follow the safety requirements established under CFR49 Part 236 [1].

5 OSC Operational Scenarios

As previously stated, the OSC does not introduce new operational functionality to what is already defined for QMB and CIXL, and therefore, the operational scenarios are the same as what is defined for those systems.

The proposed architecture for QMB and FMB Office functionality achieves very loose coupling between the OSC and other Office segments, such as the PTC-BOS and PTCEA Manager. This coupling is done to make integration and interaction of the OSC with these other two PTC Office segments as simple and non-invasive as possible. This simplicity has been achieved by designing the OSC functions to operate based solely on (external) messages to and from the other Office segments. These messages are required to perform QMB/PTC functionality, with or without OSC and without requiring the OSC to access data or functions that are internal to those segments. Basically, the OSC accomplishes these functions by checking each safety-critical message produced by the PTCEA Manager or PTC-BOS to confirm that it is correct.

When the OSC detects an error, it generates and logs an event report. Each railroad, based on its needs, Office architecture, and operation specifics, can decide where the event report message is routed, e.g., PTC Help Desk, maintenance department, or CAD system. In certain cases, the dispatcher needs to be aware of events related to issues that might immediately affect safety or traffic. In a few cases, the event report also needs to go to the PTCEA Manager for it to reverse the changes made to its records, e.g., a PTCEA rollup that is rejected by the OSC. All errors detected by the OSC are stored in the OSC's log of errors with the corresponding information.

5.1 QMB Operational Scenarios

5.1.1 Train Initialization and Termination

Any and every train or railroad vehicle operating in QMB territory, either PTC-equipped or non-equipped, is monitored by the MBO and obtains a PTCEA to operate. When a train is initialized, or authorized to enter a QMB-controlled territory, the MBO is informed whether the train is capable of handling and enforcing a PTCEA. From the MBO's perspective, a train is considered enforceable (an "enforcing train") if it is communicating and its PTC onboard segment is in the ACTIVE state.

During the initialization of the Office, the OSC subscribes to the PTC-BOS to receive the following messages:

- 02003 – Selected Train ID
- 02010 – Locomotive System State
- 02050 – Authority Request
- 02070 – Onboard Violation Report
- 02072 – Onboard Violation Cleared

The process for initializing a train for operation in QMB territory leverages from existing processes in current railroad dispatching systems, based upon Train Clearance (i.e., Track Warrant for Bulletin) per the following sequence:

- When a Train Clearance is issued, CAD sends a Train Activation message to the MBO. The PTCEA Manager, OSC, and PTC-BOS all receive the message. The Train Activation message contains the Train ID and the subdivision list (list of subdivisions that the train will operate in). The MBO uses "flags" in its train records to store certain characteristics or the status of the trains.
- Upon receiving a Train Activation message for a Train ID, the PTCEA Manager creates a record for that Train ID if it will operate in a QMB-controlled territory (based on the train's subdivision list). Initially, the train record is flagged as NENC (even though it may subsequently be confirmed to be other than NENC, at which time the PTCEA Manager upgrades its status to O-PTC or QMB). A train can be initialized in the MBO well in advance of when it will start operating in a QMB territory.
- For the new train that will operate in QMB territory:
    - The OSC creates its own record for that train and flags it as NENC (even though it may subsequently be confirmed to be other than NENC, at which time the OSC upgrades its status to O-PTC or QMB).
    - The OSC validates all subsequent messages sent from the PTCEA Manager involving the created train and checks the actions are in accordance with the flags of the train in the OSC records.
    - The OSC inserts the RIC CRC into the messages if the actions are correct.
    - The OSC does not insert the RIC CRC into the message if the actions are incorrect, and informs subscribers (e.g., the CAD system) via an event report message. If something fails in the validation process, the CAD system (and/or any other subscriber to that event type, such as the maintenance department) is notified so the dispatcher can verify and rectify (if necessary) any problem with the authority issuance.
- If the train is PTC-equipped, its status changes when its onboard segment is initialized. During the initialization of a locomotive with PTC equipment on board, the step for obtaining a Train ID, implemented in the current O-PTC system, dictates the association of Train ID and Locomotive ID, both of which are confirmed by the crew upon receiving the selection options sent from the PTC-BOS. Therefore, once the association is created in the PTC-BOS after a successful onboard segment initialization, the PTCEA Manager and the OSC update the status of the train. Among other functions, the PTC-BOS is the Office component that keeps the record with the association between Train ID and Lead Locomotive (along with the OSC), while the PTCEA Manager just refers to Train ID.
- Like the PTC-BOS, the OSC creates an association between a Train ID and its Lead Locomotive ID and stores it. In all subsequent messages, the OSC validates whether the association made by the PTC-BOS matches the Train ID identified by the crew, as indicated in the message Selected Train ID (02003) sent by the train.
    - If the association is correct, the OSC inserts the RIC CRC into the message.

    - If the association is incorrect, the OSC does not insert the RIC CRC into any message between Train ID and Locomotive ID and creates the corresponding event report.

- Flags are used to specify certain characteristics of the train in the MBO records. When the PTCEA Manager updates the flags of its record for a new train that will operate in QMB territory based on the capabilities of the onboard segment, the OSC also updates its record and checks whether that Train ID is found. If the Train ID exists in the records, all subsequent messages sent from the PTCEA Manager that involve the created train are validated by the OSC which checks if the actions are in accordance with the flags of the train. If the Train ID does not exist, the OSC informs the CAD system and maintenance department, and flags the record as one of the following:
    - "QMB Train," if the train is equipped with a QMB-capable version of software on its controlling locomotive
    - "non-QMB Train," if the train is not equipped with a QMB-capable version of software on its controlling locomotive
- As the train operates (even prior to entering QMB territory), the PTC-BOS notifies the MBO when the train status changes (message 02010 – Locomotive System State). Both the PTCEA Manager and the OSC receive the message.
    - The PTCEA Manager updates the enforcing status of the train (from the Office perspective) based on train status messages (02010) and the train's communicating capability.
    - The OSC also updates the entry for a new train that will operate in QMB territory:
        - If the Train ID is found in the OSC database, the OSC stores the enforcing status of the train
        - If the Train ID is not found in the OSC database, the OSC does not confirm the enforcing condition of the train and creates, logs, and publishes the appropriate event report

When a train is terminated in the CAD system, the MBO is informed; hence, both PTCEA Manager and OSC are informed.

- Upon receiving a Train Termination message from CAD, the PTCEA Manager marks that train as terminated in its records.
- The OSC:
    - Marks the train as terminated if that Train ID is found in its records
    - If the Train ID is not found, the OSC creates, logs, and publishes the appropriate event report

5.1.2 PTCEA Issuance

The QMB Office spawns PTCEAs from the CAD-MAs. The MBO creates a PTCEA for every train that needs to enter, exist, or operate in QMB territory. The PTCEAs are exclusive, meaning they do not overlap to provide the basis for collision protection (with warnings to the crew as well as enforcement), even at Restricted Speed. While most PTCEAs have the same movement

authority limits as their "parent" CAD-MAs, a PTCEA's limits differ from those of the CAD-MA when the CAD-MA overlaps with that of another train. In the case of trains operating under unidirectional authority in a following move or in a joint work authority, the CAD-MAs may overlap, and the QMB system parses the CAD-MA into non-overlapping PTCEAs for the trains that share CAD-MA limits.

The following sequence of events is based on a CAD-MA request from the CAD system:

- Triggered by the dispatcher or movement router/planner, CAD sends a CAD-MA message for a train to the PTCEA Manager and to the OSC.
- The PTCEA Manager checks for overlap of the CAD-MA limits with the limits of any other active PTCEA in the PTCEA Manager database (with limits in subdivision/milepost format).
    - If there is no overlap, the PTCEA Manager forwards the CAD-MA message to the PTC-BOS for conversion into a PTCEA (1051) message.
    - If there is an overlap, the PTCEA Manager truncates the "To" limit of the new PTCEA to eliminate the overlap and then stores and forwards the truncated CAD-MA message (pre-PTCEA) to the PTC-BOS for conversion into a PTCEA (1051) message.
- The PTC-BOS processes/transforms the pre-PTCEA (1051) message per the following:
    - The "To" and "From" limits of the pre-PTCEA are transformed from subdivision/milepost format into block/offset format (for use in computing the HMAC).
    - The locomotive IDs associated with the Train ID contained in the PTCEA are identified and the message is addressed to the train's controlling locomotive ID.
    - The original PTCEA format (e.g., XML) is converted to the EMP format and includes the EMP header.
    - A HMAC is computed for the entire application-level message contents.
- The PTC-BOS sends the PTCEA (1051) EMP message to the OSC (not to ITCM).
- The OSC checks the PTCEA (1051) EMP message for consistency with the CAD-MA, and if an inconsistency is found, it discards the PTCEA and creates, logs, and publishes the appropriate event report. All safety-critical fields in a PTCEA that are derived from a CAD-MA are checked for the following potential inconsistencies:
    - Overlap with other train/locomotive PTCEA
    - "To" or "From" limit is outside of parent CAD-MA limits
    - PTCEA type is inconsistent with parent CAD-MA
    - PTCEA direction is inconsistent with parent CAD-MA
    - The train does not exist in OSC records
    - Limits outside of QMB territory
    - "After arrival" condition not met

- "Do not foul" condition not met
- Restriction inconsistent with parent CAD-MA
- "Stop short" inconsistent with parent CAD-MA
- QMB or O-PTC train is not in the ACTIVE state

- The OSC validates the transformations made by the PTC-BOS (i.e., block/offset format, Locomotive ID and EMP) and, if an inconsistency is found, it discards the PTCEA and creates, logs, and publishes the appropriate event report.
- The OSC checks for the overlap of the PTCEA limits with limits of any other active PTCEA in the OSC database (with limits in block/offset format), and if an overlap is found, the OSC discards the PTCEA and creates, logs, and publishes the appropriate event report.
- If the OSC detects no overlap of limits with an active PTCEA of any other train in the OSC database (with limits in block/offset format), and there are no inconsistency with the parent CAD-MA and no transformations errors, then the OSC:
  - Computes a RIC CRC over the PTCEA contents
  - Inserts the RIC CRC into the PTCEA
  - Stores the PTCEA with its limits in block/offset format
  - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS for transmission to the train

5.1.3 PTCEA Rollup

As trains move, they roll up their PTCEAs and inform the Office. The section of track being released when a PTCEA rollup occurs can be granted to other trains that receive operation authorization from CAD. If a following train has an overlapping CAD-MA on the section of track that has just been released, the MBO can automatically extend its PTCEA, and the following steps take place:

- The PTC-BOS receives a train's PTCEA rollup (02050) message and forwards it to both the PTCEA Manager and OSC.
- The PTCEA Manager and OSC process the train's PTCEA rollup (including computing a new error check code for the PTCEA with the rolled up "From" limit) and store the PTCEA update for that train. If there is a following train, the PTCEA Manager can then extend its PTCEA, invoking the process described in Section 5.3.
- The PTCEA Manager sends the extended PTCEA for the following train to the OSC.
- The OSC checks the following train's extended PTCEA for overlap with any PTCEA in its database.
  - If no overlap:
    - The OSC updates the train's PTCEA in the OSC PTCEA Active database and informs the PTCEA Manager.

        - The OSC computes and inserts a RIC CRC in the extended PTCEA.
    - If overlap (i.e., not OK):
        - The OSC creates, logs, and publishes the appropriate event report.
        - The OSC and PTCEA Manager discard the extended PTCEA and retain the prior PTCEA for the following train.

5.1.4 Following Moves

Two trains are considered to be in a following move operation in QMB territory when both trains are moving in the same direction on the same route segment, their CAD-MAs overlap, and there is no other train or PTCEA between them. When a pair of trains operate in a following move, a PTCEA rollup of the leading train in the pair causes the PTCEA Manager to automatically extend the following train's PTCEA "To" limit to the "From" limit of the leading train. A train can be simultaneously in both a following role to a train ahead and a leading role to a train behind.

When a leading train rolls up its PTCEA, the MBO can extend the following train's PTCEA accordingly but is limited to the following train's CAD-MA "To" limit. If the PTCEA rollup of the leading train indicates that it was done with a functioning VRTL, the following train's PTCEA can be extended without restricting the speed of the leading train's "From" limit, contingent on the following train having information that the tracks up to the leading train's "From" limit have no rail breaks. If the PTCEA rollup of the leading train indicates that it was not done with VRTL, the PTCEA extension of the following train has to operate at a Restricted Speed in an occupied block, if it has been granted permission from CAD to enter a block not reporting "Clear." When a QMB following train operates under an active PTCEA indicating that the leading train is not reporting functioning VRTL, the MBO also prevents the train from entering the nearest block ahead that is not reporting "Clear" within the PTCEA limits, unless the specific following train is granted permission from CAD to enter a block not reporting "Clear."

The following steps occur during following move operation:

- When the PTCEA Manager identifies that a pair of trains in a following move operation has overlapping unidirectional CAD-MAs with no other train having a PTCEA to operate between them, the Manager sets the flag for the train ahead as "Leading" and the flag for the train behind as "Following" and notifies the OSC.
- The OSC validates the following move association of the pair of trains, verifying that:
    - The leading train has an active unidirectional PTCEA
    - The following has an active unidirectional PTCEA in the same direction
    - The CAD-MAs of the two trains overlap
    - No other train's PTCEA is between them
- If the following move association is determined to be valid, the OSC updates the status in its records. Otherwise, the OSC creates, logs, and publishes the appropriate event report.
- When the PTCEA Manager identifies that the CAD-MA of the following train of a pair in following move operation no longer overlaps with the CAD-MA of the leading train, the Manager notifies the OSC that the pair is no longer in a following move operation.

- The OSC validates the removal of the following move operation associated with the pair of trains.
  - If the removal is correct, the OSC updates the status.
  - If the removal is incorrect, the OSC creates, logs, and publishes the appropriate event report.
- Upon validating the rollup of an active PTCEA from a leading train (Section 5.4), the PTCEA Manager and OSC extend the following train's PTCEA "To" limit (Section 5.3), indicating in the PTCEA whether or not the leading train ahead reported having functioning VRTL.
- Upon receiving a message from the CAD authorizing a specified QMB train designated as a following train to enter and move at Restricted Speed in a block ahead not reporting "Clear" within the train's active unidirectional PTCEA, and the train's PTCEA contains an indication that the leading train is not reporting functioning VRTL, the PTCEA Manager:
  - Uses the corresponding authority type when issuing subsequent PTCEA (01051) messages to the following train, authorizing the train to enter and move at Restricted Speed in blocks meeting these criteria
  - Sends the pre-PTCEA to PTC-BOS
- The PTC-BOS converts the pre-PTCEA (01051) message to EMP format performing the same transformations described in Section 5.1.2 and sends it to the OSC.
- The OSC performs the same validations in the PTCEA (01051) EMP message described in Section 5.1.2 and:
  - If there is no overlap and no inconsistency, the OSC:
    - Computes an RIC CRC over the PTCEA contents
    - Inserts the RIC CRC into the PTCEA
    - Stores the PTCEA with its limits in block/offset format
    - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format, including RIC) to the PTC-BOS for transmission to the train
  - If there is an overlap or inconsistency, the OSC creates, logs, and publishes the appropriate event report.
- Upon receiving a message from CAD canceling/voiding an existing authorization that is not reporting "Clear" for an identified QMB train to enter a block ahead within its active PTCEA limits, and that PTCEA indicates that the leading train is not reporting functioning VRTL, the MBO creates a pre-PTCEA message to the identified train that:
  - Cancels its authorization to enter a block ahead within its active PTCEA limits that is not reporting "Clear" when that PTCEA indicates that the leading train is not reporting functioning VRTL
  - Reinstates the Stop targets at the entrance to occupied blocks that are normally self-imposed by the onboard segment in these circumstances

- The PTC-BOS converts the pre-PTCEA message to EMP format performing the same transformations described in Section 5.1.2 and sends it to the OSC.
- The OSC performs the same validations in the PTCEA (01051) EMP message as described in Section 5.1.2.
    - If there is no overlap and no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format, including RIC) to the PTC-BOS for transmission to the train
    - If there is an overlap or inconsistency, the OSC discards the PTCEA and creates, logs, and publishes the appropriate event report.

5.1.5 PTCEA Modification/Cancellation

A PTCEA Modification or Cancellation is initiated by a request from the CAD system, i.e., a CAD-MA Modification/Cancellation. Based on the CAD-MA Modification/Cancellation, the MBO modifies the train's PTCEA and sends it to the train.

When a CAD-MA Modification is issued, the following sequence occurs:

- When the CAD system issues a PTCEA Modification, the message is sent to both the PTCEA Manager and OSC.
- Upon receiving a request from the CAD system to modify an active CAD-MA, the PTCEA Manager stores, checks for overlaps (parses the CAD-MA if necessary), and forwards the authority to the PTC-BOS for conversion into a PTCEA (1051) message with Reason for Sending = 2 (Modification of existing authority).
- The PTC-BOS processes/transforms the pre-PTCEA message per the following:
    - Transforms the "To" and "From" limits of the pre-PTCEA from subdivision/milepost format into block/offset format
    - Identifies the Locomotive ID associated to the Train ID contained in the PTCEA
    - Converts the original pre-PTCEA format (e.g., XML) to EMP format and includes the EMP header
    - Computes a HMAC based on the entire application-level message contents
- The PTC-BOS sends the PTCEA (1051) EMP message to the OSC (not to ITCM).
- The OSC performs the same validations in the PTCEA (01051) EMP message as described in Section 5.1.2.
    - If there is no overlap and no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA

        - Stores the PTCEA with its limits in block/offset format
        - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS for transmission to the train
    - If there is an overlap or inconsistency, the OSC discards the PTCEA and creates, logs, and publishes the appropriate event report.

When a CAD-MA Cancellation is issued, the following sequence occurs:

- When the CAD system issues a CAD-MA Cancellation, the message is sent to both the PTCEA Manager and OSC.
- Upon receiving a request from the CAD system to cancel an active CAD-MA, the PTCEA Manager stores and forwards the CAD-MA Cancellation message to the PTC-BOS.
- The PTC-BOS processes/transforms the CAD-MA Cancellation into a Movement Authority Void (01053) message to cancel the PTCEA per the following:
    - Identification of the controlling Locomotive ID associated with the Train ID in the CAD-MA Cancellation request
    - Conversion of the original CAD-MA Cancellation format (e.g., XML) to EMP format, including the EMP header
    - Computation of and insertion of a HMAC based on the entire application-level message contents.
- The PTC-BOS sends the Movement Authority Void (01053) message to the OSC.
- The OSC validates the transformations made by the PTC-BOS (i.e., Locomotive ID and EMP) and, if an inconsistency is found, discards the Movement Authority Void and notifies the CAD and maintenance department of the discrepancy.
- The OSC checks the Movement Authority Void (01053) message for consistency with the CAD-MA Cancellation request.
    - If an inconsistency is found, the OSC discards the Movement Authority Void and creates, logs, and publishes the appropriate event report.
    - If no consistency is found, the OSC:
        - Computes an RIC CRC over the Movement Authority Void contents
        - Inserts the RIC CRC into the Movement Authority Void
        - Stores the PTCEA and forwards the Movement Authority Void (01053) message to the PTC-BOS for transmission to the train
- Upon receiving a Confirmation of Movement Authority Void (02053) from a train, the PTC-BOS forwards it to the PTCEA Manager and to the OSC.
- The PTCEA Manager updates the train's PTCEA status.
- The OSC checks the Movement Authority Void (02053) received from the PTC-BOS with the Movement Authority Void (01053) message for consistency.

- If there is no inconsistency, the OSC moves the voided PTCEA from the list of Active PTCEAs to the list of Archive PTCEAs.
- If there is an inconsistency, it discards the confirmation of Movement Authority Void (02053) and creates, logs, and publishes the appropriate event report.

5.1.6 Violation Report

At Office initialization, the OSC and PTCEA Manager subscribe to PTCEA rollup and violation reports. If a train violates its PTCEA (e.g., due to a PTCEA modification being issued while the train is less than braking distance away from the point where a route has been modified) when the train stops, the PTCEA Manager informs the MBO with an Onboard Violation Report (02070) and continues sending a 02070 message periodically. Upon receiving an Onboard Violation Report (02070), the MBO protects the section of track that was violated (based on the train stop location contained in the 02070 message) from being granted new or extended PTCEAs to other trains. If a currently active PTCEA had already been granted to another train that includes any portion of track that has been violated, the system also issues a PTCEA modification to that train to exclude the violated area.

If a violation occurs, the violating train may send an Onboard Violation Cleared (02072) message to the PTC-BOS when the violation is cleared (train is within its PTCEA). Upon receiving an Onboard Violation Cleared (02072) message, the MBO lifts the protection previously applied to the portion of track that had been violated by that train.

When a train issues a Violation Report (02070), the following occurs:

- The train sends an Onboard Violation Report (02070) to the PTC-BOS, indicating the section of track it occupies, in violation of its PTCEA, referred to as the "violation area."
- The PTC-BOS forwards the Violation Report to the PTCEA Manager and OSC.
- The PTCEA Manager and OSC store the Violation Report.
- The OSC and PTCEA Manager check to see if another PTCEA exists in the violation area.
- If no PTCEA exists for any other train in the violation area:
  - The PTCEA Manager protects against itself issuing a subsequent PTCEA to another train in the violation area.
  - The OSC also protects the area by not appending an RIC to any subsequent PTCEAs issued to other trains in the violation area, e.g., in case the PTCEA Manager fails or does not get a violation report from the PTC-BOS.
- If a PTCEA exists for another train in the violation area:
  - The PTCEA Manager modifies the PTCEA previously issued in the violated area (per the sequence described in Section 5.1.5) to exclude the violated area.
  - If, however, the PTCEA Manager fails to modify the existing PTCEA of the other train, the OSC:
    - Creates, logs, and publishes the appropriate event report

When a train issues a Violation Report Cleared (02072), the following occurs:

- Upon receiving a Violation Cleared (02072) message from a train indicating that it has cleared the section of track from a prior violation:
  - The PTCEA Manager lifts the protection area.
  - If no discrepancies are found, the OSC lifts the protection in its records, based on the Violation Cleared (02072) message received from the PTC-BOS.
  - Otherwise, the OSC creates, logs, and publishes the appropriate event report.
  - If a train has a CAD-MA that includes all or a portion of the track for which the protection has just been lifted, the PTCEA Manager extends that train's PTCEA per the sequence described in Section 5.2.

5.1.7 Bidirectional Authorities

Bidirectional authorities are traditionally issued using forms such as Track and Time, Track Permit, or Line 4 Track Warrant, depending upon the type of territory where is was issued. The QMB System handles exclusive bidirectional authorities in the same basic manner as O-PTC. Specifically, QMB enforces the limits of a bidirectional authority to keep unauthorized trains from entering the limits and authorized trains (e.g., work trains) from leaving the limits without authorization. The same is true for joint bidirectional authorities under Basic QMB, which also include a Restricted Speed Restriction (RSR) by rule but do not provide collision protection among joint occupants. Advanced QMB functionality provides additional protection to joint occupants. More specifically, it protects them from colliding with one another within the joint authority.

5.1.7.1 Exclusive Bidirectional Authorities

Exclusive bidirectional PTCEAs are handled in much the same manner in QMB as they are handled under O-PTC. It is possible that when an exclusive bidirectional authority is issued to a train, another train (typically a non-work train) is still in the limits but moving to clear the limits at the time the exclusive bidirectional authority is issued. The MBO does not include this portion of track in the bidirectional PTCEA until the existing train releases the track part of the exclusive bidirectional authority (rolls up its unidirectional PTCEA).

When the PTCEA Manager receives an exclusive bidirectional CAD-MA from CAD for an enforcing train, the following occurs:

- Upon receiving an exclusive bidirectional CAD-MA from CAD for an enforcing train, the PTCEA Manager creates an exclusive bidirectional PTCEA (01051) message for that train as follows:
  - If there is no other train operating inside the bidirectional authority limits with a unidirectional authority to exit those limits, the PTCEA Manager creates the bidirectional pre-PTCEA message with the same movement authority limits as the CAD-MA.
  - If there is another train operating inside the bidirectional authority limits with a unidirectional authority to exit those limits, the PTCEA Manager performs the following:

        - It creates a bidirectional pre-PTCEA message constrained to prevent overlap with the unidirectional PTCEA of the preceding exiting train.
        - If the preceding exiting train has rolled up its PTCEA for a portion of the bidirectional limits and indicates that it does not have functional VRTL, it imposes an RSR throughout the bidirectional PTCEA limits until the exiting train has rolled up its PTCEA to be totally clear of the bidirectional authority limits.
- The PTCEA Manager sends the bidirectional pre-PTCEA message to the PTC-BOS.
- The PTC-BOS processes/transforms the PTCEA message into complete 1051 format per the following:
    - Transforms the "To" and "From" limits of the PTCEA from subdivision/milepost format into block/offset format
    - Identifies the Locomotive ID(s) associated with the Train ID contained in the PTCEA
    - Converts the PTCEA from the original format (e.g., XML) to EMP format, including an EMP header
    - Computes and inserts a HMAC based on the entire application-level message contents
- The PTC-BOS sends the PTCEA (1051) EMP message to the OSC.
- The OSC checks the PTCEA (1051) EMP message for consistency with the CAD-MA ("To" and "From" limits do not exceed those of CAD-MA and directionality matches), and if an inconsistency is found or if an overlap is found with another existing PTCEA, discards the PTCEA and creates, logs, and publishes the appropriate event report.
- The OSC validates the transformations made by the PTC-BOS (i.e., block/offset format, Locomotive ID, EMP) and, if an inconsistency is found, discards the PTCEA and creates, logs, and publishes the appropriate event report.
- The OSC validates the bidirectional PTCEA created by the PTCEA Manager, verifying whether it matches the original CAD-MA request and whether there is a preceding train operating inside the work authority limits.
    - If there is no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the bidirectional PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the Office interface with ITCM) for transmission to the train
    - If there is an inconsistency, the OSC discards the PTCEA and creates, logs, and publishes the appropriate event report.
- When a preceding train that has an active unidirectional PTCEA to exit the exclusive bidirectional CAD-MA limits of another train rolls up its unidirectional PTCEA limits,

the PTCEA Manager extends the bidirectional PTCEA up to the rolled up "From" limit of the unidirectional PTCEA but not beyond the bidirectional CAD-MA limits.

- The PTC-BOS and OSC follow a similar sequence for the bidirectional PTCEA extension as described for PTCEA Modification (Section 5.1.5).
- The OSC validates the extension of the bidirectional PTCEA created by the PTCEA Manager, verifying that the PTCEA is consistent with the PTCEA rollup (no overlap) of the preceding train operating inside and exiting the bidirectional authority limits and the bidirectional CAD-MA limits.
  - If there is no inconsistency, the OSC:
    - Computes an RIC CRC over the extended bidirectional PTCEA contents
    - Inserts the RIC CRC into the PTCEA
    - Stores the PTCEA with its limits in block/offset format
    - Forwards the extension of the bidirectional PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the Office interface with ITCM) for transmission to the train
  - If there is an inconsistency, the OSC:
    - Identifies the discrepancy as event type (ID) To Be Determined (TBD)
    - Logs the event report
    - Publishes a notification (event report) as configured by the railroad for that event," and discards the extended bidirectional PTCEA (unless configured to log the message)

5.1.7.2 Joint Bidirectional Authorities

The QMB Basic functionality for joint bidirectional authorities is essentially the same as in O-PTC, i.e., enforcement of CAD-MA limits and RSR only. In Basic QMB, PTCEAs overlap for trains sharing a joint bidirectional CAD-MA, and as with O-PTC, there is no enforcement to prevent collisions among joint occupants within a joint bidirectional authority. There is a provision in the scope of the QMB system for the development of Advanced Joint Bidirectional Authority (AJBA) functionalities that would protect individual train operation limits inside a joint authority. However, these functionalities are yet to be defined and therefore are beyond the scope of this document.

When the PTCEA Manager receives a joint bidirectional CAD-MA from CAD for an enforcing train, the following occurs:

- Upon receiving a joint bidirectional CAD-MA for a train, the PTCEA Manager creates a bidirectional pre-PTCEA message for the train, conveying the same movement authority limits as its CAD-MA and having a RSR throughout the limits.
- The PTCEA Manager sends the pre-PTCEA message to the PTC-BOS.
- The PTC-BOS processes/transforms the pre-PTCEA message per the following:

    - Transforms the “To” and “From” limits of the pre-PTCEA from subdivision/milepost format into block/offset format
    - Identifies the Locomotive ID(s) associated with the Train ID contained in the PTCEA
    - Converts the PTCEA from its original format (e.g., XML) to EMP format and includes the EMP header
    - Computes a HMAC based on the entire application-level message contents
- The PTC-BOS sends the PTCEA (1051) EMP message to the OSC.
- The OSC checks the PTCEA (1051) EMP message for consistency with the CAD-MA (“To” and “From” limits do not exceed those of CAD-MA and directionality matches), and if an inconsistency is found, it:
    - Identifies the discrepancy as event type (ID) TBD
    - Logs the event report
    - Publishes a notification (event report) as configured by the railroad for that event
    - Discards the extended bidirectional PTCEA (unless configured to log the message)
- The OSC validates the transformations made by the PTC-BOS (i.e., block/offset format, Locomotive ID, and EMP) and, if an inconsistency is found, it discards the PTCEA and notifies the dispatcher via CAD and the maintenance department of the discrepancy.
- The OSC validates the joint bidirectional PTCEA created by the PTCEA Manager, verifying that it matches with the joint bidirectional CAD-MA request and no other active PTCEA overlaps the bidirectional limits except for the PTCEAs of other joint occupants of that same bidirectional PTCEA.
    - If there is no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the bidirectional pre-PTCEA message (with its limits in subdivision/milepost format) to the PTC-BOS (as the Office interface with ITCM) for transmission to the train
    - If there is an inconsistency, the OSC discards the bidirectional PTCEA request and alerts the dispatcher via CAD and the maintenance department of the discrepancy.

5.1.8 Switching Operations

It is assumed that crews use O-PTC RESTRICTED state when performing switching operations in QMB territory. As is currently the case with O-PTC RESTRICTED state, there is no enforcement or warning to keep the train from moving outside the area intended for its switching operations. There is only a prompt for the crew to confirm that the train should remain in RESTRICTED state after a certain extent of operation in that state. QMB does, however, prevent other trains from obtaining PTCEAs to enter “Switching Limits” designated by the dispatcher.

Rules for operation in QMB territory should disallow a crew to enter RESTRICTED state until the crew has confirmed that the Switching Limits have been established for the train. This ensures that the train's PTCEA includes the Switching Limits to keep other trains out of those limits.

While not mandatory, Switching Limits are typically established by the dispatcher *before* the train reaches those limits for operational efficiency. If a switching operation is requested for a train before that train has an active PTCEA that includes any track segments within the switching limits, the MBO saves the request until a PTCEA is actually being issued for all or part of the Switching Limits. Upon receiving a request for Switching Limits from the CAD system, if the active PTCEA of the train that is to perform switching does not include any track segments within Switching Limits, the MBO System stores the Switching Limit request.

When the PTCEA Manager receives a request for Switching Limits from CAD for an enforcing train, the following occurs:

- The CAD system sends a request for Switching Limits to both the PTCEA Manager and OSC.
- Upon receiving a request for Switching Limits from the CAD system, if the PTCEA Manager's records indicate that the active PTCEA of the train that is to perform switching does not include any of the track within Switching Limits, the MBO stores the Switching Limit request from the CAD system.
- Upon receiving a request for Switching Limits from the CAD system, if the OSC's records indicate that the active PTCEA of the train that is to perform switching does not include any track within Switching Limits, the OSC stores the Switching Limit request from the CAD system.
- Upon receiving a request for Switching Limits from the CAD system, if the active PTCEA of the train that is to perform switching includes the entire segment of track within Switching Limits, no other train's PTCEA overlaps with the requested Switching Limits, and the train is an enforcing train, the PTCEA Manager creates a pre-PTCEA message that:
    - Includes the entire Switching Limits (except as constrained to exclude track that falls outside of QMB territory)
    - Designates the authority segments associated with switching limits as bidirectional
    - Designates the authority segments not associated with switching limits as unidirectional (except as constrained to exclude track that falls outside of QMB territory)
    - Contains summary text indicating where Switching Limits are in effect
- The OSC verifies that the bidirectional limits in the PTCEA (01051) are consistent with the Switching Limit request sent by the CAD system and do not overlap with any other train's PTCEA.
    - If there is an inconsistency, the OSC creates, logs, and publishes the appropriate event report.
    - Otherwise, the OSC:

        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the interface with ITCM) for transmission to the train
- Upon receiving a request for Switching Limits from the CAD system, if the active PTCEA of the train that is to perform switching does not include the entire segment of track within Switching Limits and the train is an enforcing train, the PTCEA Manager creates a pre-PTCEA message that:
    - Includes the entire Switching Limits, except as constrained to:
        - Exclude track that falls outside of QMB territory
        - Exclude track that overlaps with the currently active PTCEA of any other train that has an active PTCEA that includes part of the requested Switching Limits
    - Designates the authority segments associated with switching limits as bidirectional
    - Designates the authority segments not associated with switching limits as unidirectional
    - Contains summary text indicating where Switching Limits are in effect
- The OSC verifies whether the bidirectional limits in a PTCEA (01051) created by the PTCEA Manager over Switching Limits are consistent with the Switching Limits request received from the CAD system (except as limited to exclude track that falls outside of QMB territory and to exclude track that overlaps with the currently active PTCEA of any other train that has an active PTCEA that includes part of the requested Switching Limits).
    - If there is an inconsistency, the OSC creates, logs, and publishes the appropriate event report.
    - If there is no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the interface with ITCM) for transmission to the train
- When a train for which a request for Switching Limits has been stored has its active PTCEA modified to include any of the segments of track within the stored Switching Limits, the MBO processes the stored Switching Limit request per the operations described in previous items.
- If a request for Switching Limits has been received from the CAD system, another train has an active PTCEA that includes part or all of the requested Switching Limits, and that

train subsequently rolls up its PTCEA to clear some or all of the requested Switching Limits, the PTCEA Manager creates a pre-PTCEA for the switching train that:

- Includes the entire Switching Limits, except as constrained to:
  - Exclude track that falls outside of QMB territory
  - Exclude track that overlaps with the current active PTCEA of any other train that has an active PTCEA that includes part of the requested Switching Limits
- Designates the authority segments associated with Switching Limits as bidirectional
- Designates the authority segments not associated with Switching Limits as unidirectional
- Contains summary text indicating where Switching Limits are in effect

- The OSC verifies that the bidirectional limits in a PTCEA (01051) created by the PTCEA Manager and transformed (to EMP format with limits in subdivision/milepost format) by the PTC-BOS over the Switching Limits are consistent (do not overlap) with the PTCEA rollup of a train exiting those limits.
  - If there is an inconsistency, the OSC creates, logs, and publishes the appropriate event report.
  - If there is no inconsistency, the OSC:
    - Computes an RIC CRC over the PTCEA contents
    - Inserts the RIC CRC into the PTCEA
    - Stores the PTCEA with its limits in block/offset format
    - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the interface with ITCM) for transmission to the train
- Upon receiving a request to modify a train's Switching Limits, the MBO operates per sequences previously described.

  NOTE: If the dispatcher wishes to modify the Switching Limits currently assigned to a train, the dispatcher needs to cancel the current Switching Limits and create new (modified) Switching Limits.
- Upon receiving a request from the CAD system to cancel the Switching Limits for a train, the PTCEA Manager creates a unidirectional PTCEA (01051) message for the train with:
  - The same endpoint limits as in the train's total active PTCEA
  - With the "To" and "From" limits exchanged, if the direction was changed in the message from the CAD system
  - Indication that this is a modification of the existing PTCEA (Reason for sending = 2)
  - Indication that this is a unidirectional PTCEA for all authority segments (Authority Segment Direction = 1)

    - Summary text indicating that Switching Limits are no longer in effect and that the train's PTC onboard segment should now be put into ACTIVE state, not RESTRICTING state

- The OSC verifies that the unidirectional PTCEA (01051) created by the PTCEA Manager and transformed by the PTC-BOS is consistent with the Switching Limit cancellation request from CAD.
    - If there is an inconsistency, the OSC creates, logs, and publishes the appropriate event report.
    - If there is no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the interface with ITCM) for transmission to the train

5.1.9 Handling of O-PTC Trains in QMB

QMB accommodates a train whose onboard segment has an older build of PTC software installed that does not include QMB functionality (i.e., an O-PTC train) operating in QMB territory. This situation should only exist temporarily during the period between the first release of QMB onboard software for use in revenue operations and before the last release of PTC software that does not include QMB functionality is removed from use in revenue operations. In an older software build (O-PTC, non-QMB), the onboard segment does not have any QMB-specific features so it cannot *automatically* roll up PTCEAs. This segment can, however, process and enforce PTCEAs in the same manner as Track Warrant and bidirectional authority messages (i.e., using 1051, 2050, 2052, acknowledgement, etc., messages).

PTCEAs are sent electronically to O-PTC trains (like QMB trains) in all variants of QMB territory (CTC, current of traffic, etc.), not just TWC-ABS territory. In the case of an O-PTC train, the onboard segment uses existing O-PTC Office and manual crew interaction functionality when there is a need to *request* PTCEA issuance (i.e., crew authority request), roll-up, extension, or void.

PTCEAs for O-PTC trains are handled in the same manner as the operations described in Sections 5.1.2 and 5.1.5. The PTCEA message for an O-PTC train indicates that the Authority Type is "Track Warrant/Track Authority" or "Track and Time/Track Permit" (unless a new authority type is defined that is optional). The Summary Text field could be used to indicate that the message is a "PTCEA" (e.g., rather than a track warrant or bidirectional authority). Because of this Summary Text, "PTCEA" appears on the onboard display, but the movement authority otherwise appears to the crew and the O-PTC onboard segment the same as a track warrant or bidirectional authority. The crew of an O-PTC train manually initiates (requests) the roll up of the train's PTCEA (using the same human-machine interface (HMI) actions that are used when requesting the rollup of a track warrant, sending a 2050 message to the MBO) when the train has cleared a section of track.

Furthermore, the QMB operation does not prohibit the existing crew actions associated with the 01051 message. The MBO is aware of the train type and could potentially send different crew action requests to different train types (e.g., QMB and O-PTC trains).

Upon receiving and validating a rollup request message from an O-PTC train operating in QMB territory, the MBO sends a 01051 message to the train conveying the rolled up "From" limit. The train responds with a Confirmation of Movement Authority (02052) message and when the MBO receives that message, it validates the record of the rolled up PTCEA, and it then automatically extends the PTCEA of a following train.

When an O-PTC train's crew wants to roll up their PTCEA, the following occurs:

- When the crew of an O-PTC train wants to release a portion of track behind it, the crew indicates this to the onboard segment, which then sends an Authority Request (02050) message with command type 3 (rollup of existing authority without VRTL) to the PTC-BOS.
- The PTC-BOS forwards the Authority Request (02050) message to the PTCEA Manager and OSC.
- Upon receiving an Authority Request (02050) message from an O-PTC train, the PTCEA Manager verifies that the rolled up "From" limit falls within the region between the prior "From" limit of the PTCEA and the "To" limit of the train's current PTCEA.
    - If correct (within the limits), the PTCEA Manager creates a PTCEA (01051) message for that train with the requested, rolled up "From" limit.
    - If not correct, it rejects the Authority Request and notifies the O-PTC train.
- If the PTCEA Manager creates a PTCEA (01051) message in response to an Authority Request (02050) message from an O-PTC train requesting a rollup, the OSC verifies that the PTCEA is consistent with the request.
    - If there is an inconsistency, the OSC creates, logs, and publishes the appropriate event report.
    - If there is no inconsistency, the OSC:
        - Computes an RIC CRC over the PTCEA contents
        - Inserts the RIC CRC into the PTCEA
        - Stores the PTCEA with its limits in block/offset format
        - Forwards the Switching Limits PTCEA (1051) message (with its limits in subdivision/milepost format) to the PTC-BOS (as the interface with ITCM) for transmission to the train

5.1.10 NENC Trains

The QMB System provides means for the occasional operation of a train with an onboard segment that cannot enforce or support PTC data communications with the Office. A NENC Train may have 1) a failed onboard segment, 2) an onboard segment that is communicating but is not in the ACTIVE state, or 3) an onboard segment that is not communicating or may be

unequipped with any form of PTC. For the purposes of this specification, it is assumed that if any portion of the onboard segment fails, the entire onboard segment is considered to be failed.

The CAD system creates/modifies the CAD-MAs for NENC trains in the same way that it does for enforcing trains. These CAD-MAs are sent to the MBO that creates and manages PTCEAs for them. These PTCEAs are validated by the OSC in a similar manner to PTCEAs for enforcing trains. However, unlike enforcing trains, the PTCEAs for NENC trains are exchanged with alternative communication methods between the dispatcher and the train crew. Alternative communication methods could include human voice, synthesized voice, and/or text messaging, referring to anything other than PTC (EMP) messaging over ITCM.

The System sends PTCEAs created or updated by the MBO for NENC Trains to the CAD system in a form similar to that of Track Warrants (e.g., as 1051 messages or in CAD-MA format). The CAD system displays this information to the dispatcher. The dispatcher then reads the PTCEA to the crew over voice radio or approves it to be electronically transmitted in the form of a text or synthesized voice message or any other alternative method a railroad chooses. When the dispatcher receives a PTCEA update request (such as a rollup or extension request) from a crew, the CAD system allows this information to be entered via the dispatcher HMI (or another method the railroad may choose) and passed from CAD to the MBO as a digital message, potentially in the form of a CAD-MA. If wayside signals remain operational in QMB territory, an NENC train relies on wayside signal aspects and operates with speed restrictions as defined by PTC regulations (49 CFR 236, subpart I).

In QMB territory where wayside signals are no longer operational, an absolute block is established for the operation of a NENC train. Since it is expected that wayside signals will ultimately be removed in QMB territory, operation of NENC trains in QMB territory will then use absolute block protection, which may negatively impact operations. For this and other reasons, the operation of NENC trains in QMB territory should be minimized to the extent possible.

5.1.11 Transitions Into and Out of QMB Territory

It is assumed that QMB train control will be typically deployed in select areas already established as O-PTC territory. Consequently, there will be operational scenarios where trains will transition into and out of QMB territory. To non-QMB trains, QMB territory appears similar to Overlay PTC territory (either signaled or non-signaled). As previously described, the Office handles the various train types. To QMB trains, QMB territory is indicated by the FBarDirection setting in the onboard segment track database in conjunction with information in PTCEAs.

Transitions into and out of QMB territory are handled by the CAD system and its interfaces with territories that are operated with other types of train control methods. For example, in a transition from QMB to an O-PTC territory, both with underlying field (not CIXL) interlocking, the train receives a PTCEA up to the transition from QMB to O-PTC operation, and the onboard segment does not require a PTCEA beyond that boundary but requires only WSM messages (unless the O-PTC territory is TWC-ABS, requiring a track warrant).

There are no additional use cases for OSC relating specifically to transitions into and out of QMB territory, other than validating the PTCEAs in these scenarios.

5.1.12 Train Pull-Apart

The vital process to handle cars pulling apart from a train is handled on board. A QMB train equipped with VRTL can determine when the train has potentially pulled apart and notifies the train crew for action. The onboard segment stops rolling up its PTCEA and notifies the Office. The PTCEA Manager forwards the message to the CAD system. There are no use cases for the OSC to handle in this scenario.

5.2 Operations Involving OSC Not Primarily Related to QMB or CIXL

There are additional functions beyond those specifically associated with QMB and CIXL that the OSC may perform to assure the correctness of actions performed by PTC safety-critical Office functions. These functions are related to the fail-safe handling of track bulletins and track data.

5.2.1 Track Bulletins

Under QMB operation, Track and Time, Track Permits, and Line 4 Track Warrants are handled and validated in the form of PTCEAs, however, the OSC may also perform validity checks on bulletins (i.e., temporary speed restrictions, work zones and cautionary bulletins, including changes of general orders, special instructions, or rules) to validate them before they are sent to trains.

In today's O-PTC, track bulletins are sent from the CAD to the PTC-BOS and from the PTC-BOS to trains. Under QMB, track bulletins are handled in a similar fashion to that done with CAD-MAs/PTCEAs. A track bulletin originating in the CAD is sent to both the PTC-BOS and OSC. After the PTC-BOS performs its validation/transformation, the Track Bulletin message is sent to the OSC (instead of a train), which checks it for consistency with the bulletin information from the CAD and addresses it to the trains that may need it. If correct, the OSC appends an RIC CRC and sends it to the correct trains. Alternatively, the RIC CRC could be applied by the source of the track bulletin, e.g., the CAD system, for end-to-end protection against data corruption.

In today's O-PTC system, track bulletin information is sent to trains with the use of two Locomotive-Office messages – Bulletin Dataset (01041) and Bulletin Cancellation (01043). The Bulletin Dataset message (01041) includes fields for the three types of track bulletins, i.e., Form A (temporary speed restrictions), Form B (work zones), and Form C (cautionary bulletins). The field "*track bulletin type*" in the Bulletin Dataset (01041) message indicates which type of bulletin a message contains. Bulletin Dataset messages (01041) are sent from the PTC-BOS to trains at three different types of occasions:

- During initialization, when a train receives mandatory directives, with all active track bulletins per the territories the train will operate on
- When a new bulletin is issued in the CAD system for a territory that a train is either operating or will operate
- When a train requests a particular bulletin, after finding it has missed bulletin data during the polling/synchronization process

After receiving and validating the 01041 message, the onboard segment replies with a Confirmation of Bulletin Dataset (02042) message. In the case where the message contains a description 7 = Negative Acknowledgement Message (NACK)-RIC Bulletin CRC mismatch in the Acknowledgement Indication field, the OSC does not issue or extend a PTCEA for that

specific train in the section of track affected by the bulletin until there is a positive acknowledgment of the bulletin. It is assumed the PTC-BOS will resend the message after receiving the NACK-RIC Bulletin CRC message.

In today's O-PTC system, when a bulletin is cancelled, the CAD system sends the cancellation to the PTC-BOS, and the PTC-BOS issues a Bulletin Cancellation (01043) message to the trains that are operating or that will operate on the territory where the bulletin was issued. Under QMB, the OSC also 1) receives the cancellation from the CAD system, 2) validates the message created by the PTC-BOS, and, if validated, 3) appends the RIC CRC to the message before it is sent back to the PTC-BOS and sent to the correct trains (unless the railroad has chosen to apply RIC CRC at the source of bulletins, e.g., CAD).

- The OSC receives the list of subdivisions/districts that a train will operate on (sent during train initialization or when there is a change in the train subdivision/district list to distribute to a train) from CAD and stores it.
- The OSC receives the set of track bulletins from CAD.
- When a train receives mandatory directives during initialization, a new bulletin is issued by CAD in a territory where a train is operating or will operate, or a train requests a specific bulletin (message 02041), the PTC-BOS creates a Bulletin Dataset (01041) message for that Train ID and sends it to the OSC.
- The OSC validates the Bulletin Dataset (01041) message with the data received from CAD:
    - Train ID-to-Locomotive ID transformation
    - Block Offset conversion
    - Train territory list
    - Specific Form A, Form B and Form C fields
    - EMP conversion
- If inconsistencies are found, the OSC creates, logs, and publishes the appropriate event report. If not, the OSC:
    - Computes an RIC CRC over the bulletin dataset message contents
    - Inserts the RIC CRC into the bulletin dataset message
    - Stores the bulletin dataset message
    - Forwards the Bulletin Dataset (01041) message to PTC-BOS for transmission to the train.

The process for canceling bulletins is as follows:

- When CAD issues a bulletin cancellation, the PTC-BOS creates a Bulletin Cancellation (01043) message to the trains that are operating or will operate on the territory for which the bulletin was issued and sends it to the OSC.
- The OSC validates the Bulletin Cancellation (01043) messages with the data received from CAD:

- Train ID-to-Locomotive ID transformation
- Train territory list
- EMP conversion

- If inconsistencies are found, the OSC creates, logs, and publishes the appropriate event report. If not, the OSC:
  - Computes an RIC CRC over the bulletin cancellation message contents
  - Inserts the RIC CRC into the bulletin cancellation message
  - Stores the bulletin cancellation message
  - Forwards the Bulletin Cancellation (01043) message to the PTC-BOS for transmission via ITCM to the train

5.2.2 PTC Track Database

The PTC track database contains information that is considered safety-critical, such as track location and critical features for the operation of PTC. While the PTC onboard segment uses track data, the source of vital PTC track data resides in the Office, and the OSC plays a role in assuring the correctness of that data. In the current O-PTC architecture, PTC-BOS uses track data as necessary to include it in the messages that need it. A risk with the PTC-BOS handling of the PTC track data is that the PTC-BOS could corrupt the PTC track database before sending it to a train.

This risk is mitigated by sending the OSC a copy of the PTC track data (or allow it to access the track data service). The OSC would store its own copy in a database with data protection, and whenever the PTC-BOS includes PTC track data in a message (e.g., Segment Starting Milepost field in the Bulletin Dataset (1041) message), the OSC verifies its contents and only adds the RIC CRC when they match. The OSC also has the capability to transform the original format used by CAD to the format that is sent to trains, i.e., “Subdiv file” format. Alternatively, the RIC CRC can be applied at the master source of track data for end-to-end protection.

5.2.3 PTC Office Segment Poll and Current Dataset List

In PTC, the Office Segment Poll messages (01021) are sent by the Office to each locomotive to provide information on the current set of mandatory directives and track data that are currently active in the specific territory(s) on which the train is operating or plans to operate and is registered to receive the information.

The 01022 message, Current Dataset List, is also used to provide the current list of mandatory directives and track data that should be on board for a given territory. In this case, the message is sent in response to the Request Current Dataset List (02022) message sent by a train.

Under QMB, the OSC receives from CAD and stores the list of territories on which a train will operate during its initialization. The OSC also stores the list of all mandatory directives (including all active PTCEAs) that the CAD has issued. Whenever a 01021 or a 01022 message is issued by the PTC-BOS, the OSC:

- Verifies the contents of the message, checking whether:
  - It contains the correct mandatory directives, including PTCEAs

    - The message is being sent to the correct train
    - The correct PTC track data was used
    - The EMP header is correct
- If no inconsistency is found, the OSC:
    - Calculates and inserts the RIC CRC
    - Sends the message back to the PTC-BOS for transmission
- Otherwise, the OSC creates, logs, and publishes the appropriate event report.

6 OSC Failure Modes and Responses

In principle, in the event of critical failures, the OSC functions and outputs must default to a known safe state as discussed in Section 5. If the OSC detects a discrepancy between a message generated in the Office (e.g., by the PTCEA Manager or the PTC-BOS) and the OSC's own information, it will not append a valid RIC CRC to the message, and the message will be discarded by the receiving onboard segment(s). A railroad may choose the option of logging rejected (discarded) messages on a message-by-message basis.

Because the OSC is a critical component in the process of issuing QMB train authorities, bulletins, and track data, a persistent failure of any hardware or software component that affects the capacity of the OSC to perform any of its functions should cause the railroad to downgrade its operation on the affected area (e.g., subdivision/district) to a lesser mode of train control operation. Since the proposed OSC SAC is diversity and self-checking, the downgrade occurs automatically when self-checking detects an OSC failure. The downgraded operation could signal the return to the O-PTC mode of operation or PTC operation without PTC (e.g., authority conveyed via voice radio) until OSC is restored. A decision on the type of response to OSC failures will have to be made and implemented by each railroad on their own.

If CIXL is implemented, the failure of OSC functions related to that CIXL may cause impacts to the railroad operation. If a failure affects the capability of the OSC to obtain the status of field devices and update the CAD, it may cause an operational impact, as the dispatcher may make traffic management decisions based on outdated field device status information. However, since the OSC is designed to achieve a fail-safe status for the functions that require it, the OSC does not negatively affect the safety of train operations. The interface between CIXL-O and CAD should have a mechanism that detects those types of failures (e.g., heartbeat messages, explicit/non-explicit control) to minimize such impacts.

Appendix A-1. CIXL Operation Scenarios

1 Introduction

Unlike the Basic QMB system, the functional requirements for the CIXL system have not yet been defined. Therefore, a detailed analysis of the operation of the OSC with CIXL, such as the one done in previous sections for QMB functions, is beyond the scope of this document. The following subsections describe the CIXL functionality groups that require fail-safe implementation. Consequently, these are the functions that require fail-safe validation by the OSC wherever CIXL is implemented in conjunction with QMB or FMB.

1.1 PTCEA Interpretation Function

The primary function of CIXL is to interpret PTCEAs and create commands to be sent to corresponding wayside devices in the field.

Requirements

- Every new PTCEA or PTCEA modification shall be interpreted by the CIXL-O.
- In the case of a new PTCEA, based on the results of the interpretation, CIXL-O shall create the commands for line wayside devices in accordance with the route in the PTCEA.
- CIXL-O shall send the commands to the involved CIXL-F using the available communications infrastructure.
- When a PTCEA modification occurs, CIXL-O shall create the modified commands and compare them to the commands that resulted from the interpretation of the original PTCEA.
    - If no changes are found, the commands shall not be resent to the involved CIXL-F(s).
    - If differences are found, commands shall be sent to the affected CIXL-F(s).
- The message protocol, used to send the commands, shall provide authentication and data integrity services.

1.2 Control Point Functions

1.2.1 Time Locking

With CIXL, the time locking function has two versions that have a similar purpose to the current field interlocking time locking function, i.e., basic and advanced.

The basic version of time locking is executed by the PTCEA Manager. In this case, when the dispatcher needs to modify or cancel a route, the PTCEA Manager requests the train stop. The PTCEA of a train is not modified until there is a position report that confirms the train's location and that it has stopped. Based on the location information, the PTCEA Manager either truncates the PTCEA as requested by the CAD or notifies the CAD that it is not possible to truncate the PTCEA due to the position of the train.

An optional advanced version of time locking is performed by the PTCEA Manager in conjunction with the onboard computer. The CIXL-O is not involved in the time locking

process, but the process is described here since this functionality can only be enabled when CIXL is implemented.

When the dispatcher needs to modify or cancel a route, the request is created in the CAD system and sent to the PTCEA Manager. The PTCEA Manager verifies the safety of the movement authority modification. If no safety conflict exists, the PTCEA Manager communicates its intention to modify the PTCEA to the train and queries whether the train will be able to stop at or before the location where the PTCEA will be truncated. The onboard computer estimates whether the train can stop safely based on the braking curve. If the train confirms it can stop, the onboard segment informs the PTCEA Manager and enforces a stop short of the specified location, then the PTCEA Manager truncates the former PTCEA at the specified location, and the modified PTCEA is sent to the train. In some cases, train delays associated with conventional time locking are reduced.

In the case where the train cannot stop before the new limit, its onboard display and audible warning command the crew to stop the train safely. If appropriate action is not taken by the crew, the PTC onboard segment enforces a stop, but the PTCEA is not truncated or modified before there is a message to the PTCEA Manager confirming the train has stopped and giving the location of the stopped train. This process replaces the locking timer of field IXL and provides the same protection without using a fixed timeout. Since the analogous function performed by CIXL no longer uses a timer, from this point forward, this CIXL function is referred to as "the CIXL function analogous to time locking."

Unequipped trains are commanded to stop by voice, and the crew confirms both that the train has stopped and the location of the train by voice. The OS track circuit occupancy status may be used to help verify the reported location.

Time Locking Requirements (Basic Version)

- When the PTCEA Manager receives a PTCEA truncation or PTCEA modification request, it shall verify the truncation or modification does not conflict with other PTCEAs.
- If no conflict is found, the PTCEA Manager shall send a stop request message to the train to which the PTCEA applies.
- The train shall send a position report when it has stopped.
- Based on the position report, the PTCEA Manager shall either truncate the PTCEA (if the train is within the truncated limits) or communicate to the CAD that it is not possible to truncate the PTCEA to the specified limits (if the train exceeded the truncated limits).

Time Locking Requirements (Advanced Version)

- When the PTCEA Manager receives a PTCEA truncation or PTCEA modification request, it shall verify the truncation or modification does not conflict with other PTCEAs.
- When the PTCEA Manager receives a PTCEA truncation or PTCEA modification request, it shall send an intention to truncate the PTCEA message to the train to which the PTCEA applies. Based on its braking curve, the train shall calculate if it can stop within the limits of the truncated PTCEA and send a response to the PTCEA Manager.

- If the train can stop short of the PTCEA truncation point, the PTCEA Manager shall truncate the PTCEA and send it to the train.
- If the train is not able to stop short of the PTCEA truncation point, it shall start braking until it stops and send a location report.
- The PTCEA Manager shall notify the CAD that the PTCEA cannot be truncated to the requested limits.
- The PTCEA Manager shall allow manual input of unequipped trains location information to perform the function.

1.3 Codes Out

The codes out function can be performed in two different ways when CIXL is implemented. In the first case, both involved railroads have CIXL systems that can communicate with each other at the Office level. When a train on Railroad A's track is approaching Railroad B's track, and this approach could be determined by the limit of the PTCEA, Railroad A's CIXL sends a non-vital request message to Railroad B's CIXL. Then, Railroad A's CIXL notifies Railroad B's CAD system about the request, which may or may not be authorized by the dispatcher depending on the situation. If the operation is authorized, Railroad B's PTCEA Manager creates the corresponding PTCEA for the train and Railroad B's CIXL aligns the solicited route for Railroad A's train to enter Railroad B's track.

In this same scenario, with traffic in the opposite direction (i.e., a train in Railroad B's track is approaching Railroad A's track), the process is similar with one difference. Since Railroad B controls the switch to move to Railroad A's track, when the request is authorized by Railroad A's dispatcher and a PTCEA is created to enter Railroad A's territory, a copy of that PTCEA is sent to Railroad B's PTCEA Manager for it to be aware of the authorization and proceed to line the route into Railroad A's track (this is a QMB function).

The second way to perform the codes out function is used in case one of the involved railroads does not have a CIXL system or if its CIXL systems are not interconnected. In that situation, the function remains in the field and operates as it does with conventional field interlockings.

Codes Out Requirements

- CIXL-O shall notify the CAD of an incoming request from the neighboring railroad.
- When a PTCEA is created for a train to enter Railroad A's track, the PTCEA Manager shall send a copy of the PTCEA to Railroad B's PTCEA Manager. Railroad B's PTCEA Manager shall use this PTCEA to create the corresponding PTCEA for Railroad A's track.

1.4 Request and Release Logic for Pocket Track

The pocket track control function can be performed automatically by the PTCEA Manager in conjunction with CIXL if both railroads involved have a CIXL system and they communicate between each other. The dispatcher of the foreign railroad creates a request in the CAD system for a train to enter the pocket track, and that railroad's PTCEA Manager creates a Foreign PTCEA Request in order for CIXL to be aware of the request and sends it to the neighboring CIXL system. The system notifies the owning railroad dispatcher through the CAD system, and

the dispatcher can request the route for the foreign train to enter the pocket track. It must be clear that the foreign railroad does not control any aspect of the pocket track.

In the case that just one railroad has a CIXL system or if both railroads have CIXL but no communication path exists between them, the process remains manual, as it is with conventional IXL.

Request and Release Logic for Pocket Track Requirements

- When a request is created by the dispatcher in the CAD system, the PTCEA Manager shall create a Foreign PTCEA Request.
- CIXL-O shall send the request to the neighboring CIXL-O.
- The CIXL-O that receives the request shall convey it to the CAD.

1.5 Automatic Interlockings at Diamonds

In railroad crossings at grade, if coordination exists between PTCEA Managers of the involved railroads or territories, the interlocking function can be vitally performed by the PTCEAs, and it replaces the functionality in the field. This function applies to the three types of interlockings at railroad crossing at grades, i.e., automatic, manual, and Z.

For automatic interlockings where both tracks are under QMB or FMB train control, when two trains arrive at nearly the same time, the PTCEA Manager(s) decide(s) which train will pass through the diamond first. The PTCEA Manager(s) do(es) this by allowing the PTCEA of only one train to extend into the approach track circuit until determining (by its PTCEA roll up) that the train has captured the approach circuit and subsequently cleared the diamond. This avoids a potential deadlock situation where both trains are stopped short of the diamond, and a PTCEA is granted for one train to pass through the diamond first while the automatic interlocking signals the other train to pass first.

In the case where just one of the territories operates under QMB, the function remains to be executed in the field as it is conventionally done. CIXL can provide monitoring through indications if necessary.

Automatic Interlockings at Diamonds Requirements (For automatic interlockings where both tracks are under QMB or FMB)

- The PTCEA Manager shall extend the PTCEA of only one train at a time into the approach track circuit. When the train has cleared the diamond, the PTCEA Manager shall extend the PTCEA of the train in the crossing track into the approach track circuit.
- If the intersecting territories operate under different PTCEA Managers, the PTCEA Managers shall coordinate the extension of the PTCEAs into the approach track circuits.

1.6 Manual Interlockings at Diamonds

In the case that one of the tracks does not operate under QMB, this manual interlocking function at diamonds is performed by CIXL in conjunction with the PTCEA Manager. For a train running on the QMB track, the process is largely the same as generating any other PTCEA. In the case of a train on the intersecting tracks (non-QMB), when the approach track circuit is occupied, the Object Controller sends the indication to CIXL which, in turn, notifies the CAD. The dispatcher

sees the occupancy alert and sends a CAD-MA through the diamond to the PTCEA Manager for the train on the non-QMB track. Through CIXL, the PTCEA Manager sends a command to clear the signal for trains to pass through the diamond. This command also tells the WIU to lock the WSMs for the QMB track at "Stop" for both directions until the O/S becomes occupied, and then both the approach track circuit and the O/S becomes unoccupied again. This process prevents a conflicting move, even if a train on QMB track gets a PTCEA before the train on non-QMB track clears the diamond.

The functionality of manual interlockings can be replaced by a function performed solely by the PTCEA Manager if both intersecting tracks operate with QMB. In the case that both tracks are owned by the same railroad, the authority for a train to pass through the diamond is totally handled by the PTCEA, i.e., no OC or CIXL functionality is needed.

In the case that the tracks are owned by different railroads, the PTCEA Managers of the involved railroads coordinate the issuance of non-overlapping PTCEAs in the diamond. Again, no OC or CIXL functionality is needed.

Manual Interlockings at Diamonds Requirements (One track does not operate under QMB)

- CIXL-O shall notify the CAD when the approach track circuit becomes occupied in the non-QMB track.
- After receiving a CAD MA through the diamond on the non-QMB track, the PTCEA Manager, through CIXL-O, shall send a message to command to clear the signal for trains to pass through the diamond. The message shall also command the WIU to lock the WSMs for the QMB track at "Stop" for both directions until the O/S becomes occupied and then both the approach track circuit and the O/S becomes unoccupied again.

Manual Interlockings at Diamonds Requirements (Both tracks operate under QMB or FMB)

If the intersecting territories operate under different PTCEA Managers, the Managers shall coordinate the process of issuing PTCEAs for trains to pass through the diamond.

Appendix B. Segment Requirements

Moving Block Train Control Office Safety Checker (OSC)

Segment Requirements Specification

Prepared by

Transportation Technology Center, Inc.

Version 2.0

November 22nd, 2021

The information in this document is based upon work supported by the Federal Railroad Administration under contract DTFR5311-D00008L. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the author(s) and do not necessarily reflect the views of FRA or U.S. Department of Transportation.

REVISION RECORD

VER	DESCRIPTION OF CHANGE	DATE
1.4	Draft Release	8/31/2021
2.0	Updated for final report	11/22/2021

1 Introduction

New methods of train control that have the potential to enhance safety, reliability, and operational performance have been identified and researched as part of an ongoing program to support higher reliability and capacity train control (HRCTC). The new methods build upon the existing Positive Train Control (PTC) system in the form of additional modes of operation for use in designated territories.

The HRCTC program addresses Enhanced Overlay PTC (EO-PTC), Quasi-Moving Block (QMB), and Full-Moving Block (FMB) methods of train control. In both QMB and FMB implementation, a movement authority known as a PTC Exclusive Authority (PTCEA) is provided to each train in the form of "From" and "To" limits that can be defined to any track location but not necessarily confined to fixed (block) locations. The PTCEAs are dynamically updated automatically by Office functions in a moving block manner as trains move along the track. In QMB operations, track circuits are used for broken rail detection.

In QMB, non-overlapping movement authorities, known as PTCEAs, are issued by the PTCEA Manager for every train operation, a process that offers safety improvements over current Overlay PTC (O-PTC) by including the ability to provide restricted speed collision protection, such as rear-end collision protection and, in certain configurations, collision protection within a joint authority. Taking advantage of the PTCEA concept, a spin-off from QMB, known as Centralized Interlocking (CIXL), is focused on the option to eliminate core interlocking functions of current signaling systems from the field with the addition of Office functions that would perform the functionalities eliminated in the field and vitally command wayside devices.

Both systems, QMB and CIXL, require the implementation of a group of safety-critical functions in the Office. While these functions are to be included in the PTCEA Manager and the PTC Back Office Server (PTC-BOS), to make them fail-safe, an Office Safety Checker (OSC) can be used to provide an independent real-time check that they are performed correctly. OSC functions may be implemented in an independent standalone manner or may be integrated with PTCEA Manager functionality if the PTCEA Manager is designed to be fail-safe. This document presents the Segment Requirements Specification (SegRS) for the OSC as standalone functionality.

1.1 Scope

This document specifies the proposed segment requirements for the OSC as part of the QMB or Moving Block Office (MBO) segment. It is not intended to duplicate the requirements already addressed by the QMB or other Interoperable Train Control (ITC) specifications, but rather, to define how the OSC performs functions that validate the safety-critical functions of the MBO.

In a broader vision, the OSC is the component that can provide safety-critical validation for any Office functions that require such validation, i.e., the OSC is not limited only to support MBO functionality. This specification includes the requirements necessary to satisfy the PTC-BOS functions that require safety-critical validation, including those that are not necessarily related to MBO functionality. This validation focuses on the PTC-BOS functions that process vital information to be sent from the Office to conventional PTC, referred to here as O-PTC, QMB and FMB trains (e.g., track bulletins) that have already been defined in Standard S-9361 [3] as those that need the Redundant Integrity Check (RIC) Cyclic Redundant Check (CRC). The OSC also validates vital information exchanged between the Office and trains, e.g., PTCEA

extensions and rollups. For this specification, it is assumed that O-PTC trains have the ability to process an RIC CRC.

To leave the maximum possible flexibility for each OSC supplier to develop their most effective design, the system-level requirements in this specification focus on the railroads' needs and not implementation solutions. Accordingly, the system-level requirements do not allocate functions to segments, particularly functions that could be allocated differently by different system architects. The OSC requirements in this document, on the other hand, are allocated specifically to the OSC segment.

Requirements for the implementation of FMB are being prepared in separate projects and are not included in this OSC SegRS. However, the majority of FMB Office functionality inherits QMB functions, so it is expected that only a small amount of additional functionality is envisioned when upgrading the QMB OSC segment specification to accommodate FMB as well. Once FMB requirements are fully developed, this OSC SegRS may be updated accordingly.

CIXL is an optional QMB implementation component and its system requirements have not been developed yet, thus this SegRS may require an update once CIXL functions that require OSC validation are fully developed.

1.2 Organization of the Specification and Requirements Designation

Each section of this document may contain two forms of information, i.e., narrative text and explicit requirements or goals.

The narrative text includes background information, notes, and other supplemental information to provide context and clarify the requirements. Each of the actual explicit requirements contains the word "shall" and typically follows the narrative text in a numbered or lettered list. Goals, on the other hand, contain the word "should" rather than "shall."

When necessary, requirements include existing ITC PTC message numbers as found in an Interface Control Document (ICD) and are provided within parentheses, e.g., (01051). For messages that are expected to be railroad-specific or that are for an ICD other than the Office-Locomotive ICD, a message placeholder is utilized with empty parentheses, i.e., "( )." These empty parentheses are often seen for messages between the Computer-Aided Dispatching (CAD) system and the OSC.

1.3 Document Overview

- Section 1 provides general information of the document.
- Section 2 details the OSC functional requirement specifications.
- Section 3 details the OSC non-functional requirement specifications.
- Section 4 details PTC-BOS requirements to support OSC.

2 Functional Requirements

2.1 General

The OSC requirements are leveraged from the specification of QMB system and segment requirements for the Office functions that require fail-safe implementation. The QMB requirements include a set of functions that are considered the minimum functionality to implement the QMB operation, identified as Basic QMB, which allows the operation of QMB trains that do not have Vital Rear of Train Location (VRTL) or Advanced Joint Bidirectional Authority (AJBA) in territories where conventional track circuits are implemented. The OSC requirements were developed for Basic QMB and VRTL functions. These functional requirements were expanded to include the necessary requirements for the OSC to make them fail-safe.

The primary and most fundamental purpose of the OSC for Moving Block functionality is to verify that the limits of any PTCEA issued to a train do not overlap with the active PTCEA limits of any other train (with the exception of a case related to joint work authorities in an optional simplified implementation of QMB, or Basic QMB).

In order to validate additional safety-critical functions, the OSC will acquire most of the same input information that other MBO components (e.g., PTCEA Manager) receive to implement those functions as well as the output produced by these other components based on that input information, according to the Safety Assurance Concept (SAC) principle of diversity and self-checking [2]. For example, if a CAD Movement Authority (CAD-MA) is sent from the CAD to the PTCEA Manager, resulting in a PTCEA creation or update, the OSC will receive the same CAD-MA from the CAD system to verify whether the PTCEA Manager produced a PTCEA that agrees with the input data. Similarly, when the train onboard segment rolls up a PTCEA and the PTCEA Manager processes and updates that train's PTCEA (and eventual PTCEA extension to other trains), the OSC needs to receive the PTCEA rollup message issued by the train onboard segment to verify that the subsequent PTCEA extension is safe. When a requirement states that a message is received by the OSC either from the onboard segment or from the PTCEA Manager, it is assumed that the message passed through the PTC-BOS.

The OSC also includes safety-validation features for certain O-PTC Office functionalities. To develop these requirements, it is assumed that the O-PTC onboard computer capability for handling RIC CRCs will be implemented for onboard QMB software.

When the OSC detects an error, it generates and logs an event report. Event reports should be time-stamped and may include additional information as needed to support troubleshooting, e.g., message ID, source, and destination (if the event was detection of a problem in a message). Each railroad, based on its needs, office architecture, and operation specifics, can decide where the event report message is routed, e.g., PTC Help Desk, maintenance department, or CAD system. In certain cases, the dispatcher needs to be aware of events related to issues that might immediately affect safety or traffic. In a few cases, the event report also needs to go to the PTCEA Manager to reverse the changes made to its records, e.g., a PTCEA rollup that is rejected by the OSC. All errors detected by the OSC are stored in the OSC's log of errors with the corresponding information.

2.2 External OSC Interfaces

Because the OSC is intentionally designed to work with any PTCEA Manager and PTC-BOS treated as "black boxes," the OSC does not require any internal interface with other MBO segments." This interfacing is accomplished by designing the OSC to monitor only what other Office segments send and receive over their external interfaces.

To a practical extent, the QMB system, including the OSC, uses the same ITC PTC message types and formats as O-PTC, as defined in Standard S-9361 [3], with minimal modifications in some instances.

- OSC 2.2.a-1: [OSC-1] The OSC shall interface with the CAD segment using the same interface protocols currently used by the railroad's CAD to interface with the PTC-BOS, except for differences explicitly defined by requirements in this specification.
    - NOTE: If the CAD uses an explicit/non-explicit control protocol on the interface with PTC-BOS, MBO functions will use that same protocol to interface with the CAD.
- OSC 2.2.a-2: [OSC-2] The OSC shall interface with PTC-BOS using the same interface protocols currently used by the railroad's CAD to interface with the PTC-BOS, except for differences explicitly defined by requirements in this specification.
    - NOTE: If CAD uses an explicit/non-explicit control protocol on the interface with PTC-BOS, MBO functions will use that same protocol to interface with PTC-BOS.
- OSC 2.2.b-1: [OSC-3] The OSC shall subscribe to the PTC-BOS segment with the following list of messages received by the PTC-BOS segment from the onboard segment of a communicating train:
    - 02003: Selected Train ID
    - 02010: Locomotive System State
    - 02011: Departure Test Report
    - 02040: Confirmation of Crew Acknowledgement of Bulletin
    - 02042: Confirmation of Bulletin Dataset
    - 02043: Confirmation of Bulletin Cancellation
    - 02050: Authority Request
    - 02052: Confirmation of Movement Authority
    - 02053: Confirmation of Movement Authority Void
    - 02070: Onboard Violation Report
    - 02072: Onboard Violation Cleared
    - 02080: Locomotive Position Report

2.3 Train Initialization

The following requirements are associated with the initialization of a QMB train (i.e., a train with a software version that includes QMB functionality). A QMB train can operate in any of the following PTC territory types: QMB, O-PTC, EO-PTC, and non-PTC. However, a QMB train can only perform QMB functions when operating in QMB territory. Since QMB is an enhanced version of O-PTC, a QMB train is initialized as part of the O-PTC initialization process.

Whether equipped with an ACTIVE PTC onboard segment or not, any train or railroad vehicle operating in QMB territory must be monitored by the MBO segment and obtain a PTCEA to operate. When a train is initialized on or is authorized to enter a QMB-controlled territory, the MBO segment must determine whether the train is capable of handling and enforcing a PTCEA. The OSC validates the process to identify the QMB or PTC capabilities of a train. From the MBO segment's perspective, a train is considered enforceable (an "enforcing" train) if the MBO is communicating with the train's PTC onboard segment and that onboard segment is in the ACTIVE state.

The process for initializing a train for QMB operation leverages existing processes in the railroad's current dispatching and PTC systems, based on Train Clearance (or Track Warrant for Bulletins), per the following sequence:

- When a Train Clearance is issued, CAD will send a Train Activation message to the MBO segment. The Train Activation message will contain the Train ID and the subdivision/district list (list of subdivisions/districts on which the train will operate). The CAD may send a Train Activation message for any train that receives a Train Clearance. The MBO segment is responsible for verifying whether that train will operate in a QMB territory, simplifying the process in CAD, and eliminating the need for CAD to keep track of which territories are QMB enabled.
- Upon receiving a Train Activation message for a Train ID, the MBO segment creates an entry for that Train ID if it will operate in a QMB-controlled territory (based on the train's territories list). Initially, the train is flagged as non-enforcing, non-communicating (NENC). A train can be initialized in the MBO segment well ahead of when it will start operating in a QMB territory.
- If the train is equipped, its status changes when its onboard segment is initialized. During the initialization of a locomotive with PTC equipment on board, the step for "Obtain Train ID" dictates the association of the Train ID and the Locomotive ID, both of which are confirmed by the crew upon receiving the selection options sent from the PTC-BOS. Therefore, once the association is created in the PTC-BOS after a successful onboard segment initialization, the MBO segment updates the train status flags. The OSC, as part of the MBO segment, supervises the correct update of the train information and/or flags.

The PTC-BOS is the Office component that keeps the record with the association between the Train ID and the lead locomotive, while the MBO segment generally refers to just the Train ID; however, the OSC also validates that the PTC-BOS has correctly associated the Train ID with the Locomotive ID.

As the train operates (even prior to entering a QMB territory), the PTCEA Manager updates its record of the enforcing condition of the train (from the Office perspective) based on the train

status messages (02010) and the train's communicating capability, and the OSC performs the same action so that both components have the same information.

As a train is terminated in the CAD system, it informs the MBO, which, in turn, will flag that Train ID as terminated.

- OSC 2.3.a-1: [OSC-4] Upon receiving a Train Activation message from CAD, the OSC shall:
  - Create a record for that train in the list of Train IDs containing the Train ID received in the train activation message, if the train's territories list includes QMB territory.
  - Flag the record for the Train ID as "NENC"
    - NOTE: The information stored in a train's record by the OSC includes the Train ID and its associated territories list.
    - NOTE: The train entry will never be empty. It will contain at least the default flag "NENC." This initial flag condition can be changed once the train's onboard segment is initialized and the onboard software version is determined, as well as the onboard system status as described in requirements OSC-5 and OSC-8.
- OSC 2.3.b-1: [OSC-5] Upon receiving a successful Departure Test Report (2011) message from the process of initializing the onboard segment of a train, the OSC shall:
  - Flag the record for that Train ID as a "QMB Train" if the train is installed with a QMB-capable version of software on its controlling locomotive
  - Flag the record for that Train ID as a "non QMB Train" if the train is not equipped with a QMB-capable version of software on its controlling locomotive
  - Assign Event ID OSC-EVNT-01, log it, and publish an event report message ( ) as configured by the railroad for that event type, if that Train ID is not found in its records
    - NOTE: The software versioning process is specified in the QMB System level requirements document. The process will show how a train's onboard software is determined to be either QMB-capable or not.
- OSC 2.3.b-2: [OSC-6] Based on the onboard software version, the OSC shall maintain the record for that Train ID to indicate which optional QMB software functions exist in the train, if any.
- OSC 2.3.c-1: [OSC-7] Upon receiving a Select Train ID (02003) message, the OSC shall:
  - Associate the Train ID with the corresponding Locomotive ID, if the Train ID is found in its records
  - Assign Event ID OSC-EVNT-02, publish an event report message ( ) as configured by the railroad for that event type, and log it, if the Train ID is not found in its records
  - Log the Select Train ID (02003) message along with the Event ID, if configured to do so for this event type.
- OSC 2.3.d-1: [OSC-8] Upon receiving a Locomotive System State (02010) message, the OSC shall:

- Update the Train ID record with the enforcing status of the message, if the Train ID is found in the OSC records
- Assign Event ID OSC-EVNT-03, log it, and publish an event report message ( ) as configured by the railroad for that event type, if the Train ID is not found in its records
- Log the Locomotive System State (02010) message along with the Event ID, if configured to do so for this event type, if the Train ID is not found in its records

- OSC 2.3.e-1: [OSC-9] Upon receiving a ( ) message from the CAD System notifying that a train has been terminated, the OSC shall:
  - Mark the Train ID as terminated in the list of Train IDs, if found in the records
  - Assign Event ID OSC-EVNT-04, log it, and publish an event report message ( ) as configured by the railroad for that event type, if the Train ID record is not found

2.4 PTCEA Issuance

The MBO spawns PTCEAs from CAD-MAs. Except for the case of Basic QMB, in which multiple trains operate under the same joint work authority where AJBA has not yet been implemented, PTCEAs are exclusive, meaning they do not overlap. This concept forms the basis for the QMB to provide collision protection (with warnings to the crew as well as enforcement), even at Restricted Speed. While most PTCEAs have the same movement authority limits as their "parent" CAD-MAs, a PTCEA's limits will differ from those of the CAD-MA when the CAD-MA overlaps with that of another train. The CAD-MAs may overlap in the case of trains operating under unidirectional authority in a following move where signals are relied on for train separation or in a joint work authority. In these cases, the QMB system parses the CAD-MA into the non-overlapping PTCEAs for the trains that share CAD-MA limits. The OSC validates that the PTCEAs issued by the PTCEA Manager do not overlap (except for the case of multiple trains operating under the same joint work authority under Basic QMB).

When two or more QMB trains follow one another closely on the same route segment and both have unidirectional authority, the QMB System automatically rolls up the PTCEA of the leading train to its rear-end location at a higher frequency than would otherwise be required. This is done in order to allow the authority of the following train to be extended before causing it to have to brake earlier than would be required under O-PTC operations (without QMB). In other words, the QMB system does not cause headways to extend beyond those enforced under O-PTC operations. The OSC validates the leading train rollup messages and the extension of the following train's PTCEA performed by the PTCEA Manager.

One exception to the requirement of exclusivity for PTCEAs is in the case of PTCEAs issued to different trains operating under the same joint bidirectional CAD-MA in the early (Basic) variant of QMB implementation. These PTCEAs are also validated by the OSC.

The OSC validates PTCEAs and inserts RIC CRC in the associated messages for all types of trains, i.e., QMB and non-QMB. It is assumed that O-PTC trains have the capability to process RIC CRC in messages received from the Office.

- OSC 2.4.a-1: [OSC-10] The OSC shall maintain a list of Active PTCEAs.

- OSC 2.4.a-2: [OSC-11] The OSC shall maintain an Archive of previously Active PTCEAs.
- OSC 2.4.b-1: [OSC-12] The OSC shall maintain a list of Active CAD-MAs.
- OSC 2.4.b-2: [OSC-13] The OSC shall maintain an Archive of previously Active CAD-MAs.
- OSC 2.4.c-1: [OSC-14] The OSC shall maintain a log of events.
- OSC 2.4.c-2: [OSC-99] All error codes and involved messages must be included in each stored error.
- OSC 2.4.d-1: [OSC-15] When storing a PTCEA in the OSC's List of Active PTCEAs or the OSC's PTCEA Archive, the OSC shall store the entire content of the PTCEA (01051) message.
- OSC 2.4.d-2: [OSC-100] All CRCs and HMACs must be included in each stored message.
- OSC_2.4.e-1: [OSC-16] The OSC shall store the contents of a CAD-MA received from the CAD system.
- OSC 2.4.e-2: [OSC-17] Upon receiving a PTCEA (01051) message from the PTC-BOS, the OSC shall validate that:
    - The PTCEA conforms with the specified format of a Movement Authority Dataset (01051) message
    - The track authorized by the PTCEA is within QMB territory
    - The PTCEA includes the parent CAD-MA authority number concatenated with an additional (child) number to distinguish it from the CAD-MA and from other PTCEAs spawned from the same CAD-MA
    - The PTCEA indicates the same directionality as the parent CAD-MA (e.g., bidirectional, unidirectional, and "To" vs. "From" limits oriented the same as in the CAD-MA for a unidirectional CAD-MA)
    - The association of Train ID with Locomotive ID is correct
    - Transforms the "To" and "From" limits of the PTCEA from the subdivision/milepost format into the block/offset format (for use in computing the HMAC) to match the transformations performed by the OSC
    - The authority limits of the PTCEA do not exceed the authority limits of the train's CAD-MA, and the authority limits of the PTCEA do not include track that overlaps with the active exclusive PTCEA of any other train
    - The authority limits of the PTCEA do not include track that falls outside of QMB territory
    - The authority limits of the PTCEA do not include Protected Tracks

        - NOTE: A Protected Track is a section of track that is not included in any active PTCEA but is occupied by a train that violated its PTCEA limits. See Section 2.8 for details.
    - The PTCEA includes, at a minimum, the track in QMB territory that may be currently occupied by the train to which it is addressed (if the train is already in QMB territory)
    - The recipient train has confirmed the reception of all active bulletins in the PTCEA's section of track via the PTC poll/sync process
    - There is a corresponding new CAD-MA request for that train, if the PTCEA is a new PTCEA (Reason for sending = 1)
    - There is a corresponding CAD-MA modification request for that train, or the train is a following train, if the PTCEA is a modification or cancellation (Reason for sending = 2)
    - The PTCEA is for a following train and indicates Authority Type = 13 = PTCEA without VRTL on leading train, if the leading train's last PTCEA rollup does not indicate it has functioning VRTL and the following train is a QMB train.
        - NOTE: Section 2.6 describes the concepts and requirements for a train to be flagged as "leading" and/or "following."
    - The PTCEA is for a following train and indicates Authority Type = 14 = PTCEA with VRTL on leading train, if the following train is a QMB train and the leading train is a QMB train where the last PTCEA rollup indicated it has functioning VRTL
    - The PTCEA indicates Authority Type = 15 if the train is a QMB following train and there is a CAD System authorization for the following train to enter and move at Restricted Speed in a block ahead within the following train's active unidirectional PTCEA
    - The PTCEA indicates Authority Type = 13 if the train is a QMB following train and the OSC has received a request from CAD to cancel a previous CAD authorization to enter a block ahead within its active PTCEA limits that is not reporting Clear
- OSC 2.4.e-3: [OSC-18] If the PTCEA satisfies the validation criteria described in [OSC-17], the OSC shall:
    - Store the train's current Active PTCEA in the OSC's PTCEA Archive, if the train has a prior PTCEA in the OSC's list of Active PTCEAs
    - Delete the train's current active PTCEA from the OSC's List of Active PTCEAs, if the train has a prior PTCEA in the OSC's list of Active PTCEAs
    - Store the new PTCEA in the OSC's List of Active PTCEAs
    - Calculate and insert an RIC CRC into the PTCEA (01051) message, if the Train ID is that of an enforcing communicating train
    - Send the PTCEA (01051) message back to the PTC-BOS to be sent to the train, if the Train ID is that of an enforcing communicating train

- Send a message ( ) containing the PTCEA to the CAD System, if the Train ID is that of a NENC train
  - NOTE: The dispatcher will communicate PTCEAs to a NENC train's crew.

- OSC 2.4.e-4: [OSC-19] if the PTCEA (01051) message fails any of the verification criteria described in [OSC-17], the OSC shall:
  - Assign Event ID OSC-EVNT-05, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the PTCEA message along with the Event ID, if configured to do so for this event type
    - NOTE: The PTCEA Manager needs to know about the event so it can perform the adequate corrective actions, e.g., in the case of the rejection of a PTCEA. For a train entering QMB territory, the PTCEA Manager would remove the PTCEA from its list of Active PTCEAs. In the case of a new PTCEA for a train already in QMB territory, the PTCEA Manager may need to restore a previously archived PTCEA to be the train's Active PTCEA.
    - NOTE: The PTC-BOS needs to know about the event so it can perform the necessary actions regarding the message, e.g., discontinue waiting for a PTCEA confirmation.
- OSC 2.4.f-1: [OSC-20] When a train clears the limits of an Active PTCEA, the OSC shall archive that PTCEA.
  - NOTE: A train may have more than one Active PTCEA at a given moment (e.g., when moving from a unidirectional to a bidirectional authority) and the OSC should only archive a PTCEA in such case when its limits are cleared by the train.
- OSC 2.4.g-1: [OSC-21] Every To Be Configured (TBC)_1 minute, the OSC shall request a list of the ID of every active train that is currently in QMB territory or that includes QMB territory within an unambiguously-defined portion of its route and is within TBC_2 minutes of entering QMB territory from the CAD System.
  - NOTE: An "unambiguously-defined portion of a route" is a portion of a route for which switch positions have been planned by the CAD System.
- OSC 2.4.g-2: [OSC-22] Upon receiving a ( ) message from the CAD System with the ID list of every currently active train that includes QMB territory within its route, the OSC shall:
  - Compare the CAD list with the PTCEAs in the OSC's list of Active PTCEAs
  - If the CAD list contains a Train ID that does not have a PTCEA in the OSC's list of Active PTCEAs:
    - Request the CAD system to resend the train activation message for that train
    - Request the current CAD-MA for that Train ID from the CAD System
      - NOTE: The CAD list must include information whether the train is equipped with a PTC onboard segment or not.

        - NOTE: The OSC must initially store a new train as NENC until PTC-BOS conveys message 02011 or 02010 from trains informing about their status.
- OSC 2.4.g-3: [OSC-23] Unless operating under Switching Limits, when a QMB train's onboard segment sends a rollup (02050) message to the MBO Segment indicating that it has cleared QMB territory at the "To" limit of its active unidirectional PTCEA, the OSC shall:
    - Designate the PTCEA as "void"
    - Store the voided PTCEA in the OSC's PTCEA Archive list
    - Delete the PTCEA from the OSC's List of Active PTCEAs
- OSC 2.4.h-1: [OSC-24] Once a train is issued a new CAD-MA, has cleared the limits of its prior CAD-MA, and there is no longer an active PTCEA for any portion of the prior CAD-MA limits, the OSC shall:
    - Store the prior CAD-MA in the OSC's CAD-MA Archive list
    - Delete the prior CAD-MA from the OSC's list of Active CAD-MAs

2.5 Rolling Up PTCEAs

A QMB train automatically rolls up its unidirectional PTCEA at a rate that the System can adjust to in real time as conditions change. When a train rolls up its PTCEA, the MBO receives the rollup message and updates its record of the train's PTCEA with the new "From" limit.

When a PTCEA rollup is issued by an Active train, a 02050 message is sent to the PTC-BOS, which then processes and forwards it to both the PTCEA Manager and OSC. Both the PTCEA Manager and OSC process it independently and update their PTCEA records. This concept follows the SAC principle of diversity where each segment (PTCEA Manager and OSC) processes information independently. A PTCEA rollup for a NENC train is handled between the dispatcher and the train crew, and when it is updated in the CAD system, the CAD system sends a PTCEA rollup message to both the PTCEA Manager and the OSC, both of which will process the PTCEA rollup independently, as done for an Active train.

The OSC verifies that the PTCEA rollup fulfills predetermined parameters.

- OSC 2.5.a-1: [OSC-25] Upon receiving a PTCEA rollup (02050) message from the PTC-BOS or a PTCEA rollup ( ) message from CAD, the OSC shall validate that:
    - The PTCEA to be updated is Active
    - The PTCEA is unidirectional
    - The new "From" limit falls within the region between the PTCEA's prior "From" limit and the PTCEA's "To" limit minus the train's length and safety margin, in the direction that produces a length of track shorter than the pre-rolled up PTCEA length
    - The information about the VRTL status of the train does not conflict with the known functionality of the train's onboard software, as determined in [OSC-6]
- OSC 2.5.a-2: [OSC-26] If a PTCEA rollup message meets the validation criteria described in [OSC-25], the OSC shall:

- Store the pre-rolled up PTCEA in the OSC's PTCEA Archive
- Delete the pre-rolled up PTCEA from the OSC's List of Active PTCEAs
- Store the PTCEA with the rolled up "From" limit along with its revised CRC and/or HMAC in the OSC's List of Active PTCEAs

- OSC 2.5.a-3: [OSC-27] If a PTCEA rollup message does not meet the validation criteria described in [OSC-25], the OSC shall:
  - Assign Event ID OSC-EVNT-06, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the PTCEA rollup message along with the Event ID, if configured to do so for this event type
    - NOTE: The PTCEA Manager needs to know about the event so it can remove the PTCEA from its list of Active PTCEAs and restore the pre-rolled up PTCEA to its List of Active PTCEAs.
    - NOTE: The PTC-BOS needs to know about the event to use the previous Authority ID and CRC for any process needed (e.g., message 01022 Current Dataset List).

2.6 Following Moves

In the QMB system, two trains are considered to be in a following move operation when both trains have active PTCEAs moving in the same direction and their CAD-MAs overlap. When a pair of trains operate in a following move, a PTCEA rollup by the leading train in the pair triggers the MBO to automatically extend the following train's PTCEA to the "From" limit of the leading train. A train can be in a following role in relation to a train ahead and in a leading role with respect to a train behind it simultaneously. The QMB system must remove the designation of leading and following trains from a pair of trains that had been operating in a following move when the CAD-MA of the following train does not overlap with the leading train anymore.

The OSC must perform the process of tagging leading-following train pairs to adequately validate the PTCEA extensions of a "Following" train in an occupied block, since the PTCEA extension is affected by the VRTL status of its "Leading" train, as reported in its PTCEA rollups. The onboard software of a "Following" train applies the pertaining restrictions to its operations based on its PTCEA and the field information received through WSMs.

- OSC 2.6.a-1: [OSC-28] Upon receiving a CAD-MA for a train that overlaps with the CAD -MA of another train, and:
  - Both trains have an active unidirectional PTCEA derived from their overlapping CAD-MAs
  - Both CAD-MAs have the same direction of movement
  - No other train is between them
- The OSC shall:

    - Flag as “Leading” the train that is ahead of the other train in this pair of trains, based on the direction of the trains’ PTCEAs
    - Flag as “Following” the train that is behind the other train in this pair of trains, based on the direction of the trains’ PTCEAs
        - NOTE: A single Train ID can be flagged as leading and following with different train pairs if the conditions are met. Once a pair of trains are flagged as “Leading/Following” they are considered to be in a “Following Move” condition.
- OSC 2.6.b-1: [OSC-29] Upon receiving a CAD-MA ( ) message from the CAD for a train flagged as “Leading” or “Following” the OSC shall:
    - Determine whether the CAD-MA of the train still overlaps that of its following move peer
    - If the CAD MAs of both trains do not overlap, remove the leading and following flags of the trains accordingly.
        - NOTE: The handling of a PTCEA (01051) extension messages for “Following” trains is addressed in Section 2.4.

2.7 Modifying or Canceling PTCEAs

If a train’s route is modified in a way that affects its active PTCEA, field interlocking logic or an electric lock switch timer should prevent any unsafe changing of the route under or within stopping distance ahead of the train. When a route is being cancelled where and interlocking route-locking remains in operation at a control point, the wayside signals and WSMs will reflect that condition independently of PTCEAs granted to all types of trains through that control point and PTC will enforce the WSMs, particularly if they conflict with a PTCEA. If a PTCEA is modified or voided by the PTCEA Manager, the OSC validates the safety of the modified or voided PTCEA before inserting an RIC CRC and sending it to the addressed train. The crew needs to confirm the PTCEA void before the OSC and PTCEA Manager update their corresponding status of active PTCEAs.

If the OSC determines that a PTCEA Void (01053) message doesn’t meet the validation criteria, it will not insert the RIC CRC, and it will not send the message back to the PTC-BOS. This means the onboard segment will not receive the message or will not act on the PTCEA Void message if it receives the message by mistake, and therefore will not send a Confirmation of the PTCEA Void (02053) message to the Office, and the current PTCEA of the train will remain in the corresponding list of Active PTCEAs in the OSC and PTCEA Manager.

The onboard segment has the responsibility to verify that it will still have a PTCEA for the track it is occupying (or verify that it is entirely out of QMB territory) before sending a Confirmation of a PTCEA Void.

- OSC 2.7.a-1: [OSC-30] Upon receiving a CAD-MA modification ( ) message from the CAD System, the OSC shall store the contents of the message in the list of Active CAD-MAs.
    - NOTE: The handling of a PTCEA (01051) message resulting from this request is addressed in Section 2.4.

- OSC 2.7.a-2: [OSC-31] Once a train is issued a new CAD-MA, cleared the limits of its prior CAD-MA, and there is no longer an active PTCEA for any portion of the prior CAD-MA limits, the OSC shall:
  - Store the prior CAD-MA in the OSC's CAD-MA Archive
  - Delete the prior CAD-MA from the OSC's list of Active CAD-MAs
- OSC 2.7.b-1: [OSC-32] Upon receiving a CAD-MA Void ( ) message from the CAD System, the OSC shall store its contents in the list of Active CAD-MAs.
- OSC 2.7.b-2: [OSC-33] When the OSC receives a PTCEA Void (01053) message from the PTC-BOS that requires crew acknowledgement, the OSC shall validate that:
  - The PTCEA Void (01053) message includes the same authority number as the CAD-MA Void ( ) authority number
    - NOTE: The authority number of the PTCEA message is the authority number in the CAD-MA Void ( ) message concatenated with an additional (child) number.
  - The railroad standard alpha carrier code (SCAC) in the PTCEA Void (01053) message matches the railroad SCAC in the CAD-MA Void ( ) message
  - The PTCEA Void (01053) message indicates Crew Action Required = 3 = Crew acknowledge
  - The PTC Subdivision/District list in the PTCEA Void (01053) message matches the CAD-MA Void ( ) message
  - The PTC Authority reference number in the PTCEA Void (01053) message matches the current train's PTCEA in the OSC's list of Active PTCEAs
- OSC 2.7.b-3: [OSC-34] If a PTCEA Void (01053) message meets the validation criteria per requirement [OSC-33], the OSC shall:
  - Compute and insert the RIC CRC into the message
  - If the train is an enforcing train, send the PTCEA Void (01053) message to the PTC-BOS
  - If the train is NENC, send the PTCEA Void (01053) message to the CAD system
- OSC 2.7.b-4: [OSC-35] If a PTCEA Void (01053) message does not meet the validation criteria per requirement [OSC-33], the OSC shall:
  - Assign Event ID OSC-EVNT-07, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the PTCEA Void (01053) message along with the Event ID, if configured to do so for this event type
- OSC 2.7.b-5: [OSC-36] Upon receiving a Confirmation of Movement Authority Void (02053) message in response to a Movement Authority Void (01053) message where Crew Action Required = 3 = Crew acknowledge, to void an enforcing train's PTCEA, the OSC shall store it until the corresponding Crew Acknowledgment of Mandatory Directive Status (2056) message is received.

- OSC 2.7.b-6: [OSC-37] Upon receiving a Crew Acknowledgment of Mandatory Directive Status (2056) message in response to a PTCEA Void (1053) message where Crew Action Required = 3 = Crew acknowledge from the CAD system to void an enforcing train's PTCEA, the OSC shall:
  - If Crew Action = 1 = Crew accept:
    - Store the voided PTCEA in the OSC's PTCEA Archive
    - Delete the PTCEA from the OSC's List of Active PTCEAs
    - Store the CAD-MA Void ( ) message related to the PTCEA Void (01053) in the OSC's CAD-MA Archive
    - Remove the CAD-MA Void ( ) message related to the PTCEA Void (01053) from the OSC's list of Active CAD-MAs
  - If Crew Action = 2 = Crew reject:
    - Store the CAD-MA Void ( ) message related to the PTCEA Void (01053) in the OSC's CAD-MA Archive indicating that the crew rejected it
  - Remove the CAD-MA Void ( ) message related to the PTCEA Void (01053) from the OSC's list of Active CAD-MAs
- OSC 2.7.c-1: [OSC-95] When the OSC receives a PTCEA Void (01053) message from the PTC-BOS that does not require crew action, the OSC shall validate that:
  - The PTCEA Void (01053) message includes the same authority number as the CAD-MA Void ( ) authority number
    - NOTE: The authority number of the PTCEA message is the authority number in the CAD-MA Void ( ) message concatenated with an additional (child) number.
  - The railroad SCAC in the PTCEA Void (01053) message matches the railroad SCAC in the CAD-MA Void ( ) message
  - The PTCEA Void (01053) message indicates Crew Action Required = 1 = No crew action required
  - The PTC Subdivision/District list in the PTCEA Void (01053) message matches the CAD-MA Void ( ) message
  - The PTC Authority reference number in the PTCEA Void (01053) message matches the current train's PTCEA in the OSC's list of Active PTCEAs
- OSC 2.7.c-2: [OSC-96] If a PTCEA Void (01053) message meets the validation criteria per requirement [OSC-95], the OSC shall:
  - Compute and insert the RIC CRC into the message
  - If the train is an enforcing train, send the PTCEA Void (01053) message to the PTC-BOS
  - If the train is NENC, send the PTCEA Void (01053) message to the CAD system
- OSC 2.7.c-3: [OSC-97] If a PTCEA Void (01053) message does not meet the validation criteria per requirement [OSC-95], the OSC shall:

- Assign Event ID OSC-EVNT-08, log it, and publish an event report message ( ) as configured by the railroad for that event type
- Store the PTCEA Void message along with the Event ID, if configured to do so for this event type

- OSC 2.7.c-4: [OSC-98] Upon receiving a Confirmation of Movement Authority Void (02053) message in response to a Movement Authority Void (01053) message where Crew Action Required = 1 = No crew action required to void an enforcing train's PTCEA, the OSC shall:
  - If Acknowledgement Indication = 1 = Acknowledged:
    - Store the voided PTCEA in the OSC's PTCEA Archive
    - Delete the PTCEA from the OSC's List of Active PTCEAs
    - Store the CAD-MA Void ( ) message related to the PTCEA Void (01053) in the OSC's CAD-MA Archive
    - Remove the CAD-MA Void ( ) message related to the PTCEA Void (01053) from the OSC's list of Active CAD-MAs
  - If Acknowledgement Indication = 2, 3, 4, 5, 6, 7 = Any type of negative acknowledgement:
    - Store the CAD-MA Void ( ) message related to the PTCEA Void (01053) in the OSC's CAD-MA Archive indicating that the crew rejected it
    - Remove the CAD-MA Void ( ) message related to the PTCEA Void (01053) from the OSC's list of Active CAD-MAs

2.8 Violation Reports

At Office initialization, the OSC and PTCEA Manager subscribe to PTCEA rollup and violation reports. If a train violates its PTCEA (e.g., due to a PTCEA modification being issued while the train is less than braking distance away from the point where a route has been modified, or due to a train not being able to stop within its predicted braking distance), when the train stops, it informs the MBO with an Onboard Violation Report (02070) message and repeats sending a 02070 message periodically. Upon receiving an Onboard Violation Report (02070) message, the MBO protects the section of track that was violated (based on the train stop location reported in the 02070 message) from being granted PTCEAs to other trains. If the section of track that was violated is already included in the PTCEA of another train, the system also issues a PTCEA modification to that train.

If a violation occurred, the train may send an Onboard Violation Cleared (02072) message to the PTC-BOS when the violation is cleared (train is back within its PTCEA). Upon receiving an Onboard Violation Cleared (02072) message, the MBO lifts the protection previously set to the portion of track that had been violated by that train.

- OSC 2.8.a-1: [OSC-38] Upon receiving an Onboard Violation Report (02070) message forwarded from the PTC-BOS indicating that the train is no longer within the limits of its PTCEA along with identification of the current location, the OSC shall:

- Check whether there is an active PTCEA for another train in the violation area
- Based on the Point of Violation Milepost, determine whether the violation is at the "From" or "To" limit of the PTCEA
- If the violation is in the "To" limit, create a Protected Track with the limits defined by the "To" limit of the PTCEA for the train that caused the violation up to the milepost indicated by the field "Head End Milepost" in the Onboard Violation Report (02070) message
- If the violation is in the "From" limit, create a Protected Track with the limits defined by the "From" limit of the PTCEA for the train that caused the violation up to the milepost indicated by the field "Rear End Milepost" in the Onboard Violation Report (02070) message

- OSC 2.8.a-2: [OSC-39] If a PTCEA exists for another train in a Protected Track and the OSC has not received a PTCEA (01051) message from the PTC-BOS within TBC_3 seconds updating that train's PTCEA to exclude the violation area from its PTCEA limits, the OSC shall create Event ID OSC-EVNT-09, log it, and publish an event report message ( ) as configured by the railroad for that event type.
- OSC 2.8.b-1: [OSC-40] Upon receiving an Onboard Violation Cleared (02072) message forwarded from the PTC-BOS indicating that it has cleared the track outside of its PTCEA, the OSC shall remove the associated Protected Track.

2.9 Exclusive Bidirectional Authorities

In QMB, exclusive bidirectional PTCEAs are handled in basically the same manner as an exclusive bidirectional authority under O-PTC. The OSC validates the safety of the specific PTCEAs created for exclusive bidirectional authorities.

- OSC 2.9.a-1: [OSC-41] Upon receiving an exclusive bidirectional CAD-MA message ( ) from the CAD System for a train, the OSC shall store it in the OSC's list of Active CAD-MAs.
- OSC 2.9.a-2: [OSC-42] Upon receiving an exclusive bidirectional PTCEA (01051) message from the PTC-BOS, the OSC shall validate:
  - The train recipient of the message matches the train of the bidirectional CAD-MA message
  - The message conveys the same movement authority limits as the CAD-MA, except as constrained to prevent overlap with the PTCEA of another train that has a unidirectional authority to exit those limits
  - The message indicates that this is a new PTCEA (Reason for sending = 1)
  - The message indicates that this is a bidirectional PTCEA (Authority Segment Direction = 2 for all segments of the bidirectional PTCEA)
  - The bidirectional PTCEA imposes Restricted Speed Restriction (RSR) within its limits, if there is a preceding train with an active unidirectional PTCEA to exit those limits and the unidirectional PTCEA overlaps with the bidirectional PTCEA limits, and the train has not rolled up its last PTCEA indicating that VRTL was active

- The track authorized by the PTCEA is within QMB territory
- The PTCEA includes the parent CAD-MA authority number concatenated with an additional (child) number to distinguish it from the CAD-MA and from other PTCEAs spawned from the same CAD-MA
- The PTCEA indicates the same directionality as the parent CAD-MA (e.g., bidirectional, unidirectional, and To vs. From limits oriented the same as in the CAD-MA for a unidirectional CAD-MA)
- The association of Train ID with Locomotive ID is correct
- Transformations of the "To" and "From" limits of the PTCEA from the subdivision/milepost format into the block/offset format (for use in computing the HMAC) match the transformations performed by the OSC
- The authority limits of the PTCEA do not exceed the authority limits of the train's CAD-MA, and the authority limits of the PTCEA do not include track that overlaps with the active exclusive PTCEA of any other train
- The authority limits of the PTCEA do not include track that falls outside of QMB territory
- The authority limits of the PTCEA do not include Protected Tracks
  - NOTE: A Protected Track is a section of track that is not included in any active PTCEA but is occupied by a train that violated its PTCEA limits. See Section 2.8 for details.
- The PTCEA includes, at a minimum, the track in QMB territory that may be currently occupied by the train to which it is addressed (if the train is already in QMB territory)
- The recipient train has confirmed the reception of all active bulletins in the PTCEA's section of track via the PTC poll/sync process

- OSC 2.9.a-3: [OSC-43] If a bidirectional PTCEA satisfies the validation criteria stated in requirement [OSC-42], the OSC shall:
  - Compute and insert the RIC CRC into the message
    - If the train is an enforcing train, send the exclusive bidirectional PTCEA (1051) message to the PTC-BOS
    - If the train is a NENC train, send the exclusive bidirectional PTCEA to the CAD System
  - Store the bidirectional PTCEA in the OSC's List of Active PTCEAs
- OSC 2.9.a-4: [OSC-44] If a bidirectional PTCEA fails any of the validation criteria stated in requirement [OSC-42], the OSC shall:
  - Assign Event ID OSC-EVNT-10, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the PTCEA message along with the Event ID, if configured to do so for this event type

        - NOTE: The PTCEA Manager is notified so it can perform the adequate corrective actions (e.g., in the case of the rejection of a PTCEA for a train entering QMB territory, the PTCEA Manager removes the PTCEA from its List of Active PTCEAs; in the case of a new PTCEA for a train already in QMB territory, return the previous active PTCEA).
        - NOTE: The PTC-BOS is notified so it can perform any necessary actions regarding the message, e.g., stop waiting for a confirmation.

- OSC 2.9.a-5: [OSC-45] The OSC shall confirm that a train has cleared the limits of its exclusive bidirectional PTCEA using the information in the last Locomotive Position Report (02080) message before archiving an exclusive bidirectional PTCEA.
- OSC 2.9.a-6: [OSC-46] Once a train has cleared the limits of its exclusive bidirectional CAD-MA, there is no longer an active PTCEA for any portion of that CAD-MA, and a CAD-MA void message ( ) has been received from the CAD system, the OSC shall:
    - Store the exclusive bidirectional CAD-MA in the OSC's CAD-MA Archive
    - Delete the exclusive bidirectional CAD-MA from the OSC's List of Active CAD-MAs
- OSC 2.9.b-1: [OSC-47] Upon receiving a PTCEA Rollup (02050) message from a preceding train without a functioning VRTL that has an active unidirectional PTCEA to exit the exclusive bidirectional CAD-MA of another train, indicating that it has cleared the bidirectional PTCEA limits, the OSC shall store the message in a separate record (separate from the regular PTCEA Rollup record described in requirement OSC-59).
- OSC 2.9.b-2: [OSC-48] Upon receiving a bidirectional PTCEA modification (01051) message removing RSR previously imposed throughout a bidirectional exclusive PTCEA, the OSC shall:
    - If no other train has a PTCEA for any portion of the bidirectional CAD limits associated with that bidirectional PTCEA:
        - Compute and insert the RIC CRC into the message
            - If the train is an enforcing train, send the exclusive bidirectional PTCEA (1051) message to the PTC-BOS
            - If the train is a NENC train, send the exclusive bidirectional PTCEA to the CAD System
        - Store the current train's active PTCEA in the OSC's PTCEA Archive
        - Delete the current train's active PTCEA from the OSC's List of Active PTCEAs
        - Store the PTCEA in the OSC's List of Active PTCEAs
        - Remove the separate record of the PTCEA Rollup (02050) message that triggered the PTCEA (01051) message
    - Otherwise:
        - Assign Event ID OSC-EVNT-11, log it, and publish an event report message ( ) as configured by the railroad for that event type

        - Store the bidirectional PTCEA modification (01051) message along with the Event ID, if configured to do so for this event type
        - Remove the separate record of the PTCEA Rollup (02050) message that triggered the PTCEA (01051) message
            - NOTE: The PTCEA Manager is notified so it can remove the PTCEA from its list of Active PTCEAs.

- OSC 2.9.c-1: [OSC-49] Upon receiving a PTCEA Rollup (02050) message from a preceding train with a functioning VRTL that has an active unidirectional PTCEA to exit the exclusive bidirectional CAD-MA of another train, indicating that it has cleared the bidirectional CAD-MA limits, the OSC shall store the message.
- OSC 2.9.c-2: [OSC-50] Upon receiving a bidirectional PTCEA modification (01051) message from the PTC-BOS extending the limits of a bidirectional exclusive PTCEA, the OSC shall validate that:
    - No other PTCEA extends into the limits of the extended bidirectional PTCEA, and the bidirectional PTCEA does not extend beyond the bidirectional CAD-MA limits
- OSC 2.9.c-3: [OSC-51] If the exclusive bidirectional PTCEA modification (01051) message extending the limits satisfies the validation criteria in [OSC-50], the OSC shall:
    - Calculate and insert RIC CRC into the message
    - If the train is an enforcing train, send the exclusive bidirectional PTCEA (01051) message to the PTC-BOS
    - If the train is a NENC train, send the exclusive bidirectional PTCEA to the CAD System
    - Store the prior train's active PTCEA in the OSC's PTCEA Archive
    - Delete the prior train's active PTCEA from the OSC's List of Active PTCEAs
    - Store the modified PTCEA in the OSC's List of Active PTCEAs
- OSC 2.9.c-4: [OSC-52] If the exclusive bidirectional PTCEA modification (01051) message extending the limits fails any of the verification criteria in [OSC-50], the OSC shall:
    - Store the modified PTCEA along with the error code(s) in the OSC's log of error notifications
    - Send an alert message ( ) to the CAD System and maintenance including the specific error code(s) and the ID of the message to which it pertains
        - NOTE: PTCEA Manager is notified so it can remove the PTCEA from its List of Active PTCEAs.

2.10 Joint Bidirectional Authorities

The QMB System's AJBA functionality prevents collisions at Restricted Speed among joint occupants of a bidirectional CAD-MA by issuing an exclusive PTCEA to each joint occupant and dynamically updating the boundary between two trains within the joint bidirectional authority as

necessary to accommodate their required movements. For trains lacking AJBA software or VRTL, or in territories where AJBA Office functionality has not been implemented, no collision protection is provided within the bidirectional authority. In this case, QMB functionality is basically the same as in O-PTC (enforcement of bidirectional CAD-MA limits and speed restriction only) wherein the upper limit of Restricted Speed is enforced throughout a joint bidirectional authority, regardless of whether AJBA and/or VRTL are functional. This OSC SegRS contains the requirements for Basic QMB operation only, i.e., without AJBA functionality.

In Basic QMB, the OSC validates the issuance of the joint work authorities. There are two validation cases. In case one, the train that arrives first to the limits of the bidirectional authority is issued an exclusive bidirectional PTCEA while other train(s) in the area approach the limits of the authority. When a second train is close to the limits, the PTCEA for the first train is updated to be a joint bidirectional PTCEA, and the second train also receives a joint bidirectional PTCEA. In the second case, the first train receives a joint bidirectional PTCEA from the start instead of an exclusive bidirectional PTCEA, i.e., there is no need to update the train's authority from exclusive to joint.

- OSC 2.10.a-1: [OSC-53] Upon receiving a joint bidirectional CAD-MA from the CAD System for an enforcing train, the OSC shall store it.
- OSC 2.10.a-2: [OSC-54] Upon receiving a joint bidirectional PTCEA (01051) message addressed to an enforcing train from the PTC-BOS or a PTCEA update (01051) message that modifies an active exclusive bidirectional PTCEA to be joint bidirectional, the OSC shall validate that:
    - It is a bidirectional PTCEA
    - It conveys the same movement authority limits as its parent joint bidirectional CAD-MA
    - The joint bidirectional PTCEA imposes RSR throughout its limits
    - If there is already another train within the limits of the joint bidirectional PTCEA, the other train also has a joint bidirectional authority
- OSC 2.10.a-3: [OSC-55] If the joint bidirectional PTCEA (01051) message satisfies the validation criteria in [OSC-054], the OSC shall:
    - Calculate and insert RIC CRC into the message
    - Send the joint bidirectional PTCEA (1051) message to the PTC-BOS
    - Store the PTCEA in the OSC's list of active PTCEAs
- OSC 2.10.a-4: [OSC-56] If the joint bidirectional PTCEA (01051) message fails any of the verification criteria in [OSC-54], the OSC shall:
    - Assign Event ID OSC-EVNT-12, log it, and publish an event report message ( ) as configured by the railroad for that event type
    - Store the PTCEA message along with the Event ID, if configured to do so for this event type
        - NOTE: The PTCEA Manager needs to know about the event so it can remove the PTCEA from its list of Active PTCEAs.

- OSC 2.10.a-5: [OSC-57] Once a train is issued a new CAD-MA, has cleared the limits of its joint bidirectional CAD-MA, and there is no longer an active PTCEA for any portion of the prior CAD-MA limits, the OSC shall:
    - Store the joint bidirectional CAD-MA in the OSC's CAD-MA Archive
    - Delete the joint bidirectional CAD-MA from the OSC's list of Active CAD-MAs

2.11 Switching Operations

For the purposes of this specification, it is assumed that crews will use O-PTC RESTRICTED state when performing switching operations in QMB territory. As is currently the case with O-PTC RESTRICTED state, there is no enforcement or warning to keep the train from moving outside of the area intended for its switching operations. The QMB does, however, prevent other trains from entering "Switching Limits" designated by the dispatcher.

The rules for operation in QMB territory should disallow a crew to enter RESTRICTED state until they have confirmed that Switching Limits have been established for their train. This ensures that their train's PTCEA includes the Switching Limits, to keep other trains out of those limits.

While not mandatory, Switching Limits will typically be established by the dispatcher *before* the train reaches those limits, for operational efficiency. If a switching operation is requested for a train before that train has an active PTCEA that includes part or all of the track within the Switching Limits, the MBO Segment must save the request until a PTCEA is actually being issued for the area where switching is to take place.

The OSC validates that the PTCEAs issued for Switching Limits do not overlap with any other active PTCEA, and the requirements for those are detailed in Section 2.4.

- OSC 2.11.a-1: [OSC-58] The OSC shall not accept PTCEA rollup (02050) messages from a train with an active Switching Operations PTCEA.
- OSC 2.11.a-2: [OSC-101] If the OSC receives a PTCEA rollup (02050) message from a train with an active Switching Operations PTCEA, it shall:
    - Assign Event ID OSC-EVNT-19, log it, and publish an event report message ( ) as configured by the railroad for that event type
    - Store the PTCEA rollup message along with the Event ID, if configured to do so for this event type

2.12 Handling of O-PTC Trains in QMB Territory

The QMB system accommodates trains operating in QMB territory with onboard PTC software that does not include QMB functionality installed (i.e., O-PTC trains). The O-PTC (non-QMB) software does not have any QMB-specific features so it cannot *automatically* roll up PTCEAs. It can, however, process and enforce PTCEAs in the same manner as Track Warrant messages (i.e., using 01051, 02050, 02052, acknowledgement, etc. messages). PTCEAs will be sent electronically to O-PTC trains (like QMB trains) in all types of QMB territory (CTC, current of traffic, etc.), not just in Track Warrant Control (TWC) - Automatic Block Signaling (ABS) territory. In the case of an O-PTC train, the onboard segment uses existing O-PTC Office and

manual crew interaction functionality when there is need to *request* PTCEA issuance (i.e., crew authority request), roll-up, extension, or void.

Upon receiving and validating a rollup message from an O-PTC train operating in QMB territory, the MBO sends a 01051 message to the train conveying the rolled up "From" limit. The train responds with a Confirmation of Movement Authority (02052) message, and when the MBO receives the message, it validates the record of the rolled up PTCEA and can then automatically extend the PTCEA of a following train.

- OSC 2.12.a-1: [OSC-59] The OSC shall store PTCEA rollup (02050) requests from O-PTC trains.
- OSC 2.12.a-2: [OSC-60] Upon receiving a PTCEA (01051) message from the PTC-BOS with a rolled up "From" limit for an O-PTC train, the OSC shall validate that:
    - It has received a PTCEA rollup (02050) message request from that train
    - The "From" limit of the PTCEA (01051) message matches the "From" limit of the PTCEA rollup (02050) message
    - The rolled up "From" limit falls within the region between the "From" and "To" limits of the current Active PTCEA of the train
- OSC 2.12.a-3: [OSC-61] If a rolled up PTCEA (01051) message for an O-PTC train meets the validation criteria of requirement [OSC-60], the OSC shall:
    - Calculate and insert an RIC CRC into the PTCEA message
    - Send the PTCEA (01051) message to the PTC-BOS
    - Store the PTCEA (01051) message in the OSC's List of Active PTCEAs along with a flag indicating that it is "pending crew confirmation"
- OSC 2.12.a-4: [OSC-62] If the rolled up PTCEA does not meet the validation criteria, the OSC shall:
    - Keep the train's currently active PTCEA in the OSC's List of Active PTCEAs without rolling it up
    - Assign Event ID OSC-EVNT-13, log it, and publish an event report message ( ) as configured by the railroad for that event type
    - Store the PTCEA message along with the Event ID, if configured to do so for this event type
        - NOTE: The PTCEA Manager needs to know about the event so it can remove the rolled up PTCEA from its List of Active PTCEAs.
- OSC 2.12.b-1: [OSC-63] Upon receiving a Confirmation of Movement Authority (02052) message from the onboard segment of an enforcing O-PTC train conveying the crew's acknowledgement of a PTCEA, the OSC shall:
    - Validate the Train ID and PTCEA ID on the Confirmation of Movement Authority (02052) message correspond to the Train ID and PTCEA ID with pending status verification in the OSC's List of Active PTCEAs

- If the validation succeeds:
  - Store the train's pre-rolled up active PTCEA in the OSC's PTCEA Archive
  - Delete the train's pre-rolled up PTCEA from the OSC's List of Active PTCEAs
  - Remove the "pending" flag from the record of the rolled up PTCEA in the OSC's list of Active PTCEAs
- If the validation fails:
  - Keep the "pending" flag in the record of the rolled up PTCEA in the OSC's List of Active PTCEAs
  - Assign Event ID OSC-EVNT-14, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the PTCEA acknowledgement message along with the Event ID, if configured to do so for this event type
- Remove the PTCEA rollup (02050) related to the PTCEA update (01051) message from its records

2.13 Identification of NENC Trains in QMB Territory

The QMB System provides means for operation of a train either without PTC or with an onboard segment that cannot enforce or cannot support PTC data communications with the Office. A NENC Train may 1) have a failed onboard segment, 2) have an onboard segment that is communicating but is not in the ACTIVE state, 3) have an onboard segment that is not communicating, or 4) be unequipped with any form of PTC. For the purposes of this specification, it is assumed that if any portion of the onboard segment fails, the entire onboard segment is considered to be failed.

The CAD system creates/modifies the CAD-MAs for NENC trains in the same way that it does for enforcing trains. These CAD-MAs are sent to the MBO, which creates and manages PTCEAs for them, and the OSC validates these PTCEAs as well. Unlike enforcing trains, however, the PTCEAs for NENC trains are exchanged with alternative communication methods between the dispatcher and the train crew. Alternative communication methods may include human voice, synthesized voice, and/or text messaging, referring to anything other than PTC (EMP) messaging over ITCM.

If wayside signals remain operational in QMB territory, a NENC train crew relies on wayside signal aspects and operates with speed restrictions as defined by PTC regulations (49 CFR 236, subpart I [1]) and additionally must comply with the limits conveyed in its current PTCEA, similar to operation today in TWC-ABS territory. However, unlike TWC-ABS territory, PTCEAs cannot overlap, so in a following move situation, PTCEAs will need to be updated more frequently than track warrants in TWC-ABS territory.

The MBO Segment, thereby the OSC, must use Train State Change (02010) messages to update a train's enforcing capabilities from the Office perspective. The process is validated by the OSC. A 02010 message from a train indicating that the state of its onboard segment is other than ACTIVE will flag it as a NENC train.

The loss of communication between a train and the Office is currently not explicitly monitored by the PTC-BOS, requiring the MBO Segment to monitor the train's communication activity to determine whether the train has become non-communicating. The method proposed to determine such conditions includes the following:

- The MBO Segment monitors the activity of response messages sent from a train's onboard segment.
- If that train does not respond for a specified number of consecutive messages, that train is considered non-communicating.

Once a train is flagged as NENC, it must restore both conditions (i.e., communicating and onboard segment in ACTIVE state) to be handled as an enforcing train. A Locomotive System State (02010) message with ACTIVE state from a communicating train will restore that train as enforcing. To restore a non-communicating train back to communicating, the MBO Segment must listen to any message that the onboard segment the train sends when it restores its communicating capabilities. As the MBO Segment is subscribed to receive only a limited set of onboard segment messages from the PTC-BOS, the MBO Segment will change its subscription with the PTC-BOS temporarily to listen to any message from the non-communicating train. When the train restores its communicating capabilities, the MBO Segment will change its subscription with the PTC-BOS back to normal subscription.

- OSC 2.13.a-1: [OSC-64] Upon receiving a Locomotive System State (02010) message with the information that a Train ID is not operating in the ACTIVE state, the OSC shall flag this train as "non-enforcing."
- OSC 2.13.a-2: [OSC-65] Upon receiving a 02010 message forwarded from the PTC-BOS indicating that the onboard segment of a train is in ACTIVE state, the OSC shall:
    - Remove the "non-enforcing" flag of the train, if flagged
    - Subscribe with the PTC-BOS to a configurable list TBC_4 of messages from that Train ID's onboard segment, if subscribed to all onboard segment to Office messages from that Train ID
- OSC 2.13.b-1: [OSC-66] Upon failing to receive TBC_5 consecutive response messages from a Train ID, the OSC shall:
    - Flag that Train ID as "non-communicating"
    - Flag that Train ID as "unknown" regarding enforcement
    - Subscribe with the PTC-BOS to receive all onboard segment to Office messages from that Train ID

2.14 Track Bulletin Functions

Mandatory directives contain safety-critical information that the OSC can validate for handling by fail-safe functions. The OSC 1) receives bulletin messages from the PTC-BOS, 2) validates the information of specific fields, and in the case that everything is correct, 3) adds an RIC CRC to the message before it is sent to the onboard segment of a train. The onboard segment determines the message is valid if the RIC CRC is correct with regard to the message contents.

When a Bulletin is canceled, the OSC validates the Bulletin Cancellation messages created by the PTC-BOS. If the validation succeeds, the OSC inserts the RIC CRC into the messages before they are sent to the corresponding trains. After a specific amount of time has passed from the reception of the Bulletin Cancellation from the CAD, the OSC archives both the original Bulletin and the Bulletin Cancellation.

- OSC 2.14.a-1: [OSC-67] Upon receiving a ( ) message from the CAD system containing one or more track bulletins, the OSC shall store their information in the OSC's list of Bulletins.
- OSC 2.14.a-2: [OSC-68] Upon receiving a Bulletin (01041) message from the PTC-BOS, the OSC shall validate in the bulletin message that:
    - For each Bulletin Segment it contains, there is a corresponding bulletin item issued by the CAD system
    - The message has the correct EMP format
    - The Milepost limits in each Bulletin Segment are correctly transformed to Block/Offset format
    - The Train ID is correctly transformed to Locomotive ID
    - The train territories list matches the list received when the train initialized
    - If Bulletin Type = 5 = Speed Restriction:
        - The number of speed restrictions is at least 1
        - The number of speed restrictions matches the information in the Bulletin ( ) message from the CAD
        - The speed restriction matches the information in the Bulletin ( ) message from the CAD
    - The train type matches the information in the Bulletin ( ) message from the CAD
    - The Effective Time Stamp matches the information in the Bulletin ( ) message from the CAD
    - The Expire Time Stamp information in the Bulletin ( ) message from the CAD
    - The number of Bulletin Segments matches the information in the Bulletin ( ) message from the CAD
    - For each Bulletin Segment, the milepost information, name, length, and PTC Subdivision matches information in the Bulletin ( ) message from the CAD
    - If Bulletin Type = 6 = Work Zone:
        - It includes at least 1 Bulletin Segment
    - If Bulletin Type = 7 = Grade Crossing:
        - The DOT ID matches the information in the Bulletin ( ) message from the CAD
        - The number of Bulletin Segments is 0
    - If Bulletin Type = 10 = Critical Alert:

        - The Time to Comply value matches the information in the Bulletin ( ) message from the CAD
    - If Bulletin Type ≠ 5, the Direction field is 1 = Enforceable in both directions
- OSC 2.14.a-3: [OSC-69] If the Bulletin (01041) message meets the validation criteria described in [OSC-68], the OSC shall:
    - Calculate and insert RIC CRC into the message
    - Send the Bulletin (01041) message to the PTC-BOS so it can be sent to the train
    - Store and flag the bulletin as "pending"
- OSC 2.14.a-4: [OSC-70] If the Track Bulletin (01041) message does not meet the validation criteria described in [OSC-68], the OSC shall:
    - Assign Event ID OSC-EVNT-15, log it, and publish an event report message ( ) as configured by the railroad for that event type
    - Store the bulletin message along with the Event ID, if configured to do so for this event type
    - Store and flag Bulletin (message) as rejected
- OSC 2.14.b-1: [OSC-71] Upon receiving a Confirmation of Bulletin Dataset (02042) message forwarded from the PTC-BOS, the OSC shall:
    - Validate that the Bulletin Dataset (02042) message has been acknowledged by checking that the Acknowledgement Indication field description 1 = Acknowledged and track limit validation is complete
    - If the validation succeeds, OSC shall remove the "pending" flag from the message record
    - If the validation fails, OSC shall keep the "pending" flag from the message record
- OSC 2.14.c-1: [OSC-72] Upon receiving a Bulletin Cancellation ( ) message issued by the CAD system, the OSC shall store it in the OSC's list of Bulletins and flag the corresponding Bulletin in the list as "Canceled"
- OSC 2.14.c-2: [OSC-73] Upon receiving a Bulletin Cancellation (01043) message from the PTC-BOS, the OSC shall validate in the Bulletin Cancellation message that:
    - There is a corresponding Bulletin Cancellation message issued by the CAD system per requirement OSC-72
    - The message has the correct EMP format
    - The bulletin reference number matches the number in the cancellation message issued by CAD
    - The Train ID is correctly transformed to the train's Locomotive ID
- OSC 2.14.c-3: [OSC-74] If the Bulletin Cancellation validation described in [OSC-73] meets the validation criteria, the OSC shall:
    - Calculate and insert RIC CRC into the message

- Send the Bulletin Cancellation (01043) message to the PTC-BOS so it can be sent to the train

- OSC 2.14.c-4: [OSC-75] If the Bulletin Cancellation validation described in [OSC-73] does not meet the validation criteria, the OSC shall:
  - Assign Event ID OSC-EVNT-16, log it, and publish an event report message () as configured by the railroad for that event type
  - Store the Bulletin Cancellation message along with the Event ID, if configured to do so for this event type
- OSC 2.14.d-1: [OSC-76] After TBC_6 time has passed since a Bulletin Cancellation was received from the CAD, the OSC shall store the corresponding Bulletin and the Bulletin Cancellation ( ) messages in the OSC's Bulletin Archive and remove them from the OSC's list of Bulletins.

2.15 PTC Track Data

The PTC track data contains information that is considered safety-critical for the operation of PTC, such as track location, geometry, and critical features. While the PTC onboard segment uses track data, the source of vital PTC track data resides in the Office, and the OSC plays a role in ensuring the correctness of that data. In the current O-PTC architecture, PTC track data is provided to the PTC-BOS, and the PTC-BOS uses data as necessary. The potential risk with the handling of the PTC track data by the PTC-BOS is that the PTC-BOS could corrupt the PTC track data before sending it to a train. The risk is mitigated by having the OSC receive a copy of the PTC track data. The OSC stores its own copy with data protection and whenever the PTC-BOS sends PTC track data, the OSC verifies its contents and only adds the RIC CRC when they are correct. The OSC also has the capability to transform the original format used by CAD to the format that is sent to trains, i.e., "Subdiv file" format.

- OSC 2.15.a-1: [OSC-77] The OSC shall receive a copy of track data in the subdivision format.
- OSC 2.15.a-2: [OSC-78] The OSC shall store the track data in its own local database.
- OSC 2.15.b-1: [OSC-79] The OSC shall use its local copy of the track data as the trusted source in any transaction that involves track data information (e.g., data validation).
- OSC 2.15.c-1: [OSC-80] The OSC shall have the capability to transform the track data from the block/offset format to the Milepost format and vice-versa.
- OSC 2.15.d-1: [OSC-81] All messages or data to be stored in the OSC's database shall be stored with all CRCs and/or HMACs.
- OSC 2.15.d-2: [OSC-82] When retrieving information from its database, the OSC shall check that the CRCs and/or HMACs are valid.
- OSC 2.15.d-3: [OSC-83] When retrieving information from its database, if a CRC or HMAC is detected to be incorrect, the OSC shall send an alert message ( ) to maintenance including the specific error code(s).
- OSC 2.15.e-1: [OSC-84] The OSC's database shall include data redundancy features.

- OSC 2.15.e-2: [OSC-85] The OSC's database shall include non-volatility features.

2.16 PTC Office Segment Poll and Current Dataset List

In PTC, the Office Segment Poll (01021) messages are sent by the Office to each locomotive to provide information on the set of mandatory directives and track data that are currently active in the specific territory (territories) on which the train is operating or plans to operate and is registered to receive the information.

The 01022 message, Current Dataset List, is also used to provide the current list of mandatory directives and track data that should be on board for a given territory. In this case, the message is sent in response to the Request Current Dataset List (02022) message sent by a train.

Both messages include safety-critical information that the OSC validates.

- OSC 2.16.a-1: [OSC-86] The OSC shall have a record of RIC Uniqueness Index for each Train ID for each message that requires this functionality (at minimum for Office Segment Poll (01021) and Current Dataset List (01022) messages).
- OSC 2.16.a-2: [OSC-87] When a train initializes, the OSC shall be set to 0 for the RIC Uniqueness Index used for Office Segment Poll (01021) and Current Dataset List (01022) messages for that train.
- OSC 2.16.a-3: [OSC-88] When a train is terminated, the OSC shall remove the RIC Uniqueness Index records for that Train ID.
- OSC 2.16.b-1: [OSC-89] Upon receiving a new Office Segment Poll (01021) message from the PTC-BOS for a specific train, the OSC shall validate that:
    - The Train Subdivision/District List CRC matches the Train Subdivision/District List CRC stored by the OSC for that Train ID
    - The Dataset CRC for each territory in the message matches the OSC records
- OSC 2.16.b-2: [OSC-90] If the validation criteria described in [OSC-89] is met, the OSC shall:
    - Increase the RIC Uniqueness Index by 1 for the specific message
    - Update in the OSC's records the RIC Uniqueness Index value for that Train ID and message
    - Insert the RIC Uniqueness Index into the message
    - Calculate and insert Composite CRC into the message
    - Send the Office Segment Poll (01021) message to the PTC-BOS so it can be sent to the train
- OSC 2.16.b-3: [OSC-91] If the validation criteria described in [OSC-89] is not met, the OSC shall:
    - Assign Event ID OSC-EVNT-17, log it, and publish an event report message ( ) as configured by the railroad for that event type

- Store the message being validated along with the Event ID, if configured to do so for this event type

- OSC 2.16.c-1: [OSC-92] Upon receiving a Current Dataset List (01022) message from the PTC-BOS, the OSC shall validate in the message that:
  - The PTC Subdivision/District Dataset CRC is correct
  - The PTC Authority Reference Number (Active PTCEA ID) for the train is correct
  - The Dataset CRC for the PTCEA is correct
  - The PTC Bulletin Reference Number(s) is correct
  - The CRC(s) around Bulletin information is correct
  - The track data version is correct
  - The CRC(s) around track data is correct
- OSC 2.16.c-2: [OSC-93] If the validation described in [OSC-91] is successful, the OSC shall:
  - Increase the RIC Uniqueness Index by 1 for the specific message
  - Update in the OSC's records the RIC Uniqueness Index value for that Train ID and message
  - Insert the RIC Uniqueness Index into the message
  - Calculate and insert RIC CRC into the message
  - Send the Current Dataset List (01022) message to the PTC-BOS (so it can be sent to the train)
- OSC 2.16.c-3: [OSC-94] If the validation described in [OSC-91] is not successful, the OSC shall:
  - Assign Event ID OSC-EVNT-18, log it, and publish an event report message ( ) as configured by the railroad for that event type
  - Store the Current Dataset List message along with the Event ID, if configured to do so for this event type

2.17 Centralized Interlocking

Currently, QMB requirements do not include CIXL, but OSC or a similar process will need to validate specific CIXL functions if and when CIXL is implemented. These requirements can be developed along with the CIXL System Requirement Specifications.

3 Non-Functional Requirements

3.1 Performance Requirements

In general, the performance requirements for OSC are primarily for the purpose of seeing that the System allows all types of operations previously supported on the railroad under O-PTC and QMB for the territory (CTC, TWC-ABS, or Current of Traffic) without negative operational impacts.

Capacity-related performance requirements will need to be determined based on the peak size of railroad operations. Because parameters may be railroad specific, specific values have not been provided.

The core of the moving block operational rules and associated functions is built in the PTCEA Manager, which will have to satisfy broader performance requirements. Since the OSC only performs safety validation functions, it should only add a marginal processing time that has been stipulated as 0.1 second.

- OSC 3.1.a-1: [OSC-102] The OSC shall perform its validation process on a message within 0.1 second.
- OSC 3.1.b-1: [OSC-103] The OSC should utilize existing Office Segment infrastructure capacity efficiently.
- OSC 3.1.c-1: [OSC-104] The OSC shall be capable of validating TBC_7 PTCEAs plus a total of TBC_8 of all other types of transactions requiring OSC validation per minute.
    - NOTE: TBC_7 and TBC_8 are railroad specific. TBC_7 plus TBC_8 should be equal to or greater than the number required for the operation of the peak number of trains that may simultaneously operate in the railroad's total QMB and O-PTC territory per minute. The OSC should accommodate at least the same number of trains operating simultaneously as O-PTC.

3.2 Safety Requirements

Safety requirements flow from QMB requirements and OSC safety analysis into this OSC segment specification. Mitigations identified in the safety analysis are transformed into formal safety-related requirements. The OSC's sole purpose is to increase the safety integrity level of functions performed in the Office to achieve the level necessary for vital functions. This increased level of safety integrity is referred to as fail-safe and is commensurate with an overall train control system mean-time-to-hazardous-event (MTTHE) on the order of 10^9 hours. All OSC functional requirements are safety-critical requirements.

Federal requirements regarding Safety Assurance Criteria and Processes are found in 49CFR236 Subpart I, Appendix C [1]. SAC to achieve fail-safe implementation are defined in standard IEEE-1483 [2]. The requirements contained in these documents assume that the "Diversity and Self-Checking" SAC is employed. This SAC is applied to the PTCEA Manager, PTC-BOS, and OSC segments working together such that each vital function is performed in two of the three segments (one of which is always the OSC). Each of these three segments need to perform internal self-checking per the "Diversity and Self-Checking" SAC.

Upon validation of a message, the OSC applies a 32-bit RIC CRC to the message using an equation/algorithm that is different from the CRC-32 applied by the PTC-BOS, and that is unknown to the PTC-BOS.

In QMB or FMB train control systems, the PTCEAs and Track Bulletins are delivered electronically and may be the sole artifacts crews depend on for safe train operation. Therefore, the data within these messages are vital and require validation for the safety of rail network operations.

- OSC 3.2.a-1: [OSC-105] Every OSC function identified by one or more requirements in this specification is safety-critical and shall be implemented in accordance with 49CFR236 Subpart I, Appendix C when operating in conjunction with a PTC-BOS and PTCEA Manager as specified in functional requirements.
- OSC 3.2.b-1: [OSC-106] The OSC shall protect vital application data and addresses contained in a message designated as vital per S-9361 [3] against errors incurred during communications and storage.
    - NOTE: Application data contained in messages related to enforcement functions is vital. Track bulletin limits including the locations of critical assets and track geometry used by enforcing trains in QMB territory is safety-critical data.
    - NOTE: At least one 32-bit CRC should be stored with each OSC record of vital data.
    - NOTE: Critical assets include track circuits, switches, control points, and clearance points.
- OSC 3.2.c-1: [OSC-107] The OSC shall perform self-checking as required per the "Diversity and Self-Checking" SAC.

3.3 Security Requirements

The OSC is one of the MBO Segments and therefore is assumed to inherit the O-PTC and QMB security requirements and methods. It is also assumed that the PTC-BOS remains the entity that will apply HMACs to messages.

3.4 Reliability, Availability and Maintainability Requirements

The OSC is one of the MBO System Office Segments (albeit not necessarily on the same physical servers) and therefore is assumed to inherit the O-PTC Reliability, Availability, and Maintainability (RAM) Requirements for both hardware and software. Since many of its failure modes can disrupt railroad operations, the OSC must have very high availability. Implementation of the OSC may be railroad specific and it is assumed that RAM requirements will be defined on a case-by-case basis. Consequently, this section contains no requirements unique to OSC.

Aside from the above description of inheritance of O-PTC RAM requirements, this section is primarily a place holder for possible future use, e.g., for insertion of railroad-specific RAM requirements or reference to a supplemental RAM document.

3.5 Human Factors Requirements

The OSC operations are developed and designed to work and reside within the Office Segment. The OSC functionalities are an automated set of computer instructions without the need for

human interaction for normal operation. The OSC requires only a conventional human-machine interface (HMI) for system maintenance, the method of which is assumed to be railroad specific.

3.6 Environmental and Physical Requirements

The OSC is one of the MBO Segments and therefore is assumed to inherit the O-PTC Office Segment environmental and physical requirements.

3.7 Extensibility Requirements

The design and implementation of the OSC should facilitate the potential subsequent addition of functionalities beyond those specified herein with maximal reuse of QMB functionalities and loose coupling among them.

In particular, if QMB is implemented in stages, the OSC should be designed to facilitate subsequent incorporation of additional functionalities such as Advanced QMB and CIXL. Also, the OSC is intended to support FMB train control operations if and when implemented. Therefore, the OSC shall be developed to accommodate future needs in safety-critical functions in the Office.

- OSC 3.7.a-1: [OSC-108] OSC software should be designed and implemented with a modular architecture.
- OSC 3.7.b-1: [OSC-109] OSC software should be upgradeable on a modular basis with minimal or no changes to existing modules.
- OSC 3.7.c-1: [OSC-110] OSC software should be designed with maximum independence among modules (loose coupling).
- OSC 3.7.d-1: [OSC-111] The OSC System should be designed to minimize data dependencies among hardware components.

3.8 Configurable Parameters

The parameters in Table 1 are configurable and may differ from one railroad to another. Changes to the default values of these parameters may require industry approval.

Table 1. List of Configurable Parameters

TBC Identifier	TBC Description	Default Value
TBC_1	Number of minutes between OSC requests for a list of all active trains from CAD and PTC-BOS	<TBD>
TBC_2	Estimated threshold time in minutes before a train enters QMB territory and triggers the CAD System to include that train in the list of active trains in QMB territory	<TBD>
TBC_3	Maximum time in seconds that the OSC waits for a PTCEA update for a train whose PTCEA has been violated by another train	<TBD>
TBC_4	List of messages from a Train ID that the OSC subscribes in the PTC-BOS when the train's onboard segment is in active state	<TBD>
TBC_5	Number of consecutive response messages not received by the OSC that trigger the OSC to flag a train as non-communicating and enforce status unknown	<TBD>
TBC_6	Number of minutes since a Track Bulletin Cancellation ( ) message from CAD was received until the OSC archives it	<TBD>
TBC_7	Minimum number of PTCEAs that the OSC must be capable of processing per minute	<TBD>
TBC_8	Minimum number of transactions (not including PTCEAs) that the OSC must be capable of processing per minute	<TBD>

3.9 Event Reports

The list in Table 2 includes the OSC generated events. It also details the fields the event report must include.

Table 2. List of Event Reports

Event ID	Description	Fields to include in Event Report and Log
OSC-EVNT-01	Train ID from Departure Test Report (2011) not found in records	Event ID, event number, message type, message number, message time, Train ID
OSC-EVNT-02	Train ID from Select Train ID (02003) not found in records	Event ID, event number, message type, message number, message time, Train ID
OSC-EVNT-03	Train ID from Locomotive System State (02010) message not found in records	Event ID, event number, message type, message number, message time, Train ID
OSC-EVNT-04	Train ID from ( ) message from the CAD System notifying that a train has been terminated not found in records	Event ID, event number, message type, message number, message time, Train ID
OSC-EVNT-05	PTCEA (01051) message does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, field(s) that failed validation

Event ID	Description	Fields to include in Event Report and Log
OSC-EVNT-06	PTCEA rollup message does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, field(s) that failed validation
OSC-EVNT-07	PTCEA Void (01053) message that requires crew confirmation does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, crew action required, field(s) that failed validation
OSC-EVNT-08	PTCEA Void (01053) message that does not require crew confirmation does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, crew action required, field(s) that failed validation
OSC-EVNT-09	PTCEA update not received after Onboard Violation Report (02070) message	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, field(s) that failed validation (all fields related to Onboard Violation Report (2070) message.
OSC-EVNT-10	Exclusive bidirectional PTCEA (02051) message does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, authority type, field(s) that failed validation
OSC-EVNT-11	Exclusive Bidirectional PTCEA modification (01051) message removing RSR does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, authority type, field(s) that failed validation
OSC-EVNT-12	Joint bidirectional PTCEA (01051) message does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, authority type, field(s) that failed validation
OSC-EVNT-13	Rolled up PTCEA (01051) message for an O-PTC train does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, field(s) that failed validation
OSC-EVNT-14	Confirmation of Movement Authority (02052) message conveying the crew's acknowledgement of an O-PTC train's PTCEA does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, PTC authority reference number, field(s) that failed validation
OSC-EVNT-15	Track Bulletin (01041) message does not meet validation criteria	Event ID, event number, message type, message number, message time, Train ID, bulletin ID, field(s) that failed validation
OSC-EVNT-16	Bulletin Cancellation (01043) message does not meet validation criteria	Event ID, event number, message type, message number, message time, destination, bulletin ID, field(s) that failed validation
OSC-EVNT-17	Office Segment Poll (01021) message does not meet validation criteria	Event ID, event number, message type, message number, message time, destination, field(s) that failed validation
OSC-EVNT-18	Current Dataset List (01022) message does not meet validation criteria	Event ID, event number, message type, message number, message time, destination, field(s) that failed validation
OSC-EVNT-19	Crew Authority Request (02050) message does not meet validation criteria	Event ID, event number, message type, message number, message time, field(s) that failed validation

4 PTC-BOS Requirements to Support OSC

Certain system-level assumptions or pre-requisites are required for the OSC system to operate. While the PTC-BOS system is not considered part of the OSC or MBO, there are certain OSC-specific requirements for modifications that must be implemented in the PTC-BOS.

For the OSC to provide safety validation of messages, those messages need to pass between the PTC-BOS and the OSC before they are sent to the addressed onboard segment, using the ITCM infrastructure. Before sending them to a QMB train, the PTC-BOS needs to route the following messages to the OSC for safety validation:

- (01021) Office Segment Poll
- (01022) Current Dataset List
- (01041) Bulletin Dataset
- (01043) Bulletin Cancellation
- (01051) Movement Authority Dataset
- (01053) Movement Authority Void

Once the OSC determines that a message meets the validation criteria, the OSC will calculate and insert the RIC CRC or Composite CRC into the message before sending the message to the PTC-BOS to send it to the corresponding onboard segment.

If the OSC determines that a message does not meet the validation criteria, it may send a message with the invalid message's ID and an error code to the PTC-BOS. The PTC-BOS is notified so it can perform any necessary actions regarding the message, e.g., delete the message from its records, stop waiting for a confirmation, etc.

Currently in the listed messages, the message field related to the RIC functionality is populated with all zeros (hexadecimal 0000) when OSC functionality is not present in the Office. Once the OSC is implemented and active in the Office, the PTC-BOS needs to be programmed to populate the RIC CRC field of a message with a number different than zeros to make a distinction that the functionality is present but the field has not yet been populated with an RIC CRC value.

The PTC-BOS must populate the following fields in the following messages with all ones (hexadecimal FFFF) before sending the message to the OSC for validation:

- (01021) Office Segment Poll
  - Composite CRC
- (01022) Current Dataset List
  - Composite CRC
- (01041) Bulletin Dataset
  - RIC Bulletin CRC
- (01043) Bulletin Cancellation
  - RIC Bulletin Cancellation CRC

- (01051) Movement Authority Dataset
  - RIC Authority CRC
- (01053) Movement Authority Void
  - RIC Authority Void CRC

The PTC-BOS must not modify a message's RIC field once the message has been validated by the OSC (e.g., once there is a value other than 0000 or FFFF in the RIC CRC field). There could be cases where the message does not meet the validation criteria of the OSC, in which case the OSC does not insert the RIC CRC into the message and does not send the message back to the PTC-BOS. Instead, the OSC sends an alert to the PTC-BOS with the message ID to notify the PTC-BOS about the error. Based on this notification, the PTC-BOS must stop performing any subsequent action for that message, such as waiting for a confirmation or resending the message X seconds after not receiving a confirmation.

The PTC-BOS needs to send the following incoming messages from a QMB train to both the PTCEA Manager and the OSC:

- 02003: Selected Train ID – used to associate Train ID with Locomotive ID
- 02010: Locomotive System State – used to determine onboard segment enforcing status
- 02011: Departure Test Report – used to identify the train's onboard software version
- 02040: Confirmation of Crew Acknowledgement of Bulletin – used to confirm a train's crew receipt of a Bulletin
- 02042: Confirmation of Bulletin Dataset – used to confirm a train's receipt of a Bulletin
- 02043: Confirmation of Bulletin Cancellation – used to confirm a train's receipt of a Bulletin Cancellation
- 02050: Crew Authority Request – used to roll up a train's PTCEA
- 02052: Confirmation of Movement Authority – used to confirm a train's receipt of a PTCEA
- 02053: Confirmation of Movement Authority Void – used to confirm a train's receipt of a PTCEA void
- 02070: Onboard Violation Report – used to identify the location of an authority violation
- 02072: Onboard Violation Cleared – used to confirm the clearance of an authority violation
- 02080: Locomotive Position Report – used to determine the position of the train that was last reported

Appendix C. Safety Analysis

Safety Analysis Report

for the

Moving Block Trian Control Office Safety Checker (OSC)

Prepared by

Transportation Technology Center, Inc.

Version 2.0

November 22nd, 2021

The information in this document is based upon work supported by the Federal Railroad Administration under contract DTFR5311-D00008L. Any opinions, findings, and conclusions or recommendations expressed in this report are those of the author(s) and do not necessarily reflect the views of FRA or U.S. Department of Transportation.

REVISION RECORD

VER	DESCRIPTION OF CHANGE	DATE
1.0	Draft Release	8/28/2021
2.0	Updated for final report	11/22/2021

1 Introduction

New methods of train control that have the potential to enhance safety, reliability, and operational performance have been identified and researched as part of an ongoing program to support Higher Reliability and Capacity Train Control (HRCTC). The new methods build upon the existing Positive Train Control (PTC) system in the form of additional modes of operation for use in designated territories.

The HRCTC program addresses Enhanced Overlay PTC (EO-PTC), Quasi-Moving Block (QMB), and Full-Moving Block (FMB) methods of train control. In both QMB and FMB implementation, a movement authority (MA) known as a PTC Exclusive Authority (PTCEA) is provided to each train in the form of "From" and "To" limits that can be defined for any track location, not necessarily confined to fixed (block) locations. PTCEAs are dynamically updated automatically by Office functions in a moving block manner as trains move along the track. In a QMB operation, track circuits are used for broken rail detection.

The PTCEAs are issued by the PTCEA Manager for every train operation, offering safety improvements over current Overlay PTC (O-PTC) due to their exclusive (non-overlapping) nature, including the ability to provide restricted speed collision protection, such as rear-end collision protection and, in certain configurations, collision protection within a joint authority. Taking advantage of the PTCEA concept, a spin-off from QMB or FMB, known as Centralized Interlocking (CIXL), is focused on the option to eliminate the core interlocking functions of current signaling systems with the addition of Office functions that would 1) perform the functionalities eliminated in the field and 2) vitally command wayside devices. Both systems, QMB and CIXL, require the implementation of a group of safety-critical functions in the Office. While these functions are or will be included in the PTCEA Manager and the PTC-BOS to make them fail-safe, an Office Safety Checker (OSC) can be used to provide an independent real-time check to ensure the functions are performed correctly. The OSC functions may be implemented on an independent stand-alone server or may be hosted on a shared server that also performs other Office functions. This document presents the safety analysis for OSC as stand-alone functionality. CIXL is an optional implementation component, thus CIXL and QMB safety-critical functions are differentiated in this project.

2 Scope

The scope of this analysis was limited to the hazards related to the Moving Block Office (MBO) functions supported by the OSC that are different in QMB as compared with O-PTC, to the extent that safety and hazard mitigation information is available on the current O-PTC system. The safety analyses are also limited to O-PTC risks that can be mitigated with OSC functions. Further, the analyses were limited to current signaling systems (i.e., no assessment of centralized interlocking, which is a potential future option associated with QMB or FMB). The Hazard Analysis Results presented in Section 6 provide the hazard descriptions, mitigations, and risk assessment results from the analyses of QMB with OSC support.

This safety analysis is a preliminary draft that will require further updates by any railroad choosing to implement the QMB system (including OSC support) to account for railroad-specific characteristics.

3 QMB Safety/Hazard Risk Assessment Methodology

This analysis considers the hazards deemed to have changed the levels of risk, as well as the hazards that initially appeared to possibly change under QMB operations but after further assessment were found not to result in an increased risk. The QMB impacts were evaluated with respect to safety as compared with the currently approved and fielded O-PTC baseline. This analysis does not address all hazards considered during initial O-PTC Safety Plans, particularly if their level of risk clearly would not change during QMB operations.

The QMB (and FMB) Office architecture supported by the OSC employs the safety assurance concept (SAC) known as "Diversity and Self-Checking." From a functional standpoint, the OSC validates the group of QMB, potential future CIXL, and safety-critical PTC-BOS Office functions. The complete QMB and O-PTC Office functionality is performed collectively by the PTCEA Manager, CIXL, and PTC-BOS, with the OSC mitigating the risk by using diverse methods to check the result of every safety-critical Office function performed by those other Office components and provide a fail-safe response in the event of a wrong-side fault. The PTCEA Manager essentially handles PTCEA-related functions, the CIXL handles interlocking-related functions, and the PTC-BOS handles track bulletin data, track data, and message exchanges between trains and the Office.

The analysis performed was qualitative in nature according to standard safety analysis and risk assessment methods and was constrained by available information about the current O-PTC system. The assessed areas were driven by proposed changes to the O-PTC system implementation, operating rules, processes, procedures, and performance (i.e., line capacity and average velocity). The evaluated areas are listed and mentioned in the Hazard Risk Assessment Results provided in Table 2.

The safety analysis was performed from three standard perspectives culminating in a Hazard Risk Assessment (HRA). The three perspectives, summarized in the following subsections are:

1. Preliminary Hazard Analysis (PHA)
2. System Hazard Analysis (SHA)
3. Operation and Support Hazard Analysis (O&SHA)

3.1 Preliminary Hazard Analysis

The purpose of a PHA is to identify hazards, assess their potential severity, and identify potential hazard mitigations before the system design is complete. The PHA tasks include the performance and documentation of an initial safety assessment. Based on the best data available, including mishap data (if assessable) from similar systems and other lessons learned, potential hazards associated with the proposed functions are evaluated for severity and operational constraints. Potential mitigations and alternatives to eliminate hazards or reduce their associated risk to an acceptable level are included.

3.2 System Hazard Analysis

The SHA addresses hazards related to safety-critical functions that are to be implemented in subsystems. This analysis 1) identifies the hazards in more detail than the PHA, 2) assigns each hazard to one or more subsystems, 3) identifies the planned design mitigations, 4) provides assessments of the risk associated with each of the hazards (comparing mitigation efforts proposed for QMB implementation with the existing O-PTC system), and 5) estimates the residual hazard frequency or probability for use in the Hazard Risk Index (HRI). The term "residual" is used to refer to the remaining probability or risk after any mitigations have been applied.

In the SHA, a residual HRA is performed based on the severity assigned to each hazard in the PHA and the probability or frequency of that hazard after mitigations are implemented by subsystem design. The objective of the HRA is to achieve a residual risk for each hazard that is both acceptable and achievable with the proposed implementation. The HRA is based on the HRI for each hazard.

3.3 Operation and Support Hazard Analysis

The purpose of the O&SHA is to identify and assess hazards introduced by operational and support activities and procedures, as well as to evaluate the adequacy of operational and support procedures, facilities, processes, training, and equipment used to mitigate risks associated with identified hazards.

The O&SHA task builds on the SHA, and it identifies the methods planned to mitigate hazards that could not be eliminated by system design. The human is considered an element of the total system, both receiving inputs and initiating outputs within the analysis.

Like the SHA, the O&SHA identifies the hazards in more detail than the PHA, estimating the residual hazard frequency or probability necessary to complete the HRA. Rather than specifying design features to be implemented, however, the O&SHA specifies operational and support procedures, facilities, processes, training, and equipment required or planned in order to adequately mitigate hazards.

Collectively, the SHA and O&SHA specify the mitigations (at a high level) chosen to adequately mitigate all identified hazards, in order to achieve an acceptable level of risk.

3.4 Hazard Risk Assessment

Table 2 shows the HRA, which combines the results of all three safety analyses performed, namely, PHA, SHA, and O&SHA. The residual risk level assessments shown in the table are based on the collective effect of mitigations to be implemented by system (hardware or software) design (results of the SHA) and to be performed by humans (results of the O&SHA).

3.5 Hazard Risk Index

Acceptable target safety levels have been defined by railroads implementing PTC. The HRI is a tool widely used to establish a required level of integrity based on the predicted probability and severity of identified hazards. The matrix in Figure 1 shows the HRI used for the analysis of QMB from the I-ETMS PTC Development Plan (PTCDP).[3]

Severity → / Probability ↓	I Catastrophic	II Critical	III Marginal	IV Negligible
A Frequent	UN	UN	UN	AC
B Probable	UN	UN	UN	AC
C Occasional	UN	UN	AC/WR	AC
D Remote	UN	AC/WR	AC	AC
E Improbable	AC/WR	AC	AC	AC

Integrity Goal Definitions :

UN	- Unacceptable
AC/WR	- Acceptable with review by the railroad's chief safety officer or designated representative
AC	- Acceptable without review

Figure 1. Hazard Risk Index

The HRI correlates the predicted severity and probability of the occurrence of identified hazards to a risk integrity goal. The matrix is used in the HRA process to establish initial hazard risk and set priorities for resolutions that eliminate, minimize, or control the identified hazards. The HRA process combines the hazard severity and hazard probability to determine which identified hazards are:

- Acceptable as is (without officer review)
- Acceptable with review by the railroad's Chief Safety Officer or designated representative with proper documentation thereof
- Unacceptable

Hazard assessment is based on the potential impact of the hazard on personnel, facilities, equipment, operations, the public, or the environment, as well as on the product itself. Other factors specific to the product may also be used to assess risk. For a vital O-PTC system, Federal Regulations[4] mandate that sufficient documentation demonstrates that the PTC system, as built,

[3] Wabtec Railway Electronics, Union Pacific Railroad, Norfolk Southern Railway, CSX Transportation, Inc., Interoperable Electronic Train Management System (I-ETMS) Positive Train Control Development Plan (PTCDP) Version 2.0, 2011.

[4] "Positive Train Control Systems," Code of Federal Regulations, Title 49, Part 236, Subpart I, 2011.

fulfills the Safety Assurance Criteria and Processes set forth.[5] If an identified hazard cannot be eliminated, the process should reduce the associated risk to an acceptable level through design and proper implementation using safety assurance concepts.

Hazard severity is defined as a qualitative measure of the worst credible mishap resulting from personnel error, environmental conditions, design inadequacies, and/or procedural deficiencies for a system, subsystem, or component failure or malfunction, and is categorized as follows:

I. Catastrophic
   - Deaths, system loss, or severe environmental damage

II. Critical
   - Severe injury, severe occupational illness, or major system or environmental damage

III. Marginal
   - Minor injury, minor occupational illness, or minor system or environmental damage

IV. Negligible
   - Less than a minor injury, occupational illness, or less than minor system or environmental damage

Hazard probability is defined as the probability with which a specific hazard will occur during the planned lifecycle of the system element, subsystem, or component. Hazard probability can be described subjectively in potential occurrences per unit of time, events, population, items, or activity, and is ranked as follows:

A. Frequent
   - P(incident) > 1E-3 per operating hour, where "P(incident)" is shorthand for "probability of incident"
   - Classification associated with a hazardous event that is likely to occur often in the life of the system, subsystem, or component
   - Likely to occur frequently in an individual item; may be continuously experienced in fleet/inventory

B. Probable
   - 1E-3 per operating hour ≥ P(incident) > 1E-5 per operating hour
   - Classification associated with a hazardous event that will occur several times in the life of the system, subsystem, or component
   - Will occur several times in the life of an item; will occur frequently in fleet/inventory

C. Occasional
   - 1E-5 per operating hour ≥ P(incident) > 1E-7 per operating hour

[5] "Safety Assurance Criteria and Processes," in Code of Federal Regulations, Title 49, Part 236, Appendix C, 2011

- Classification associated with a hazardous event that is likely to occur sometime in the life of the system, subsystem, or component
- Likely to occur sometime in the life of an item; will occur several times in fleet/inventory

D. Remote

- 1E-7 per operating hour ≥ P(incident) > 1E-9 per operating hour
- Classification associated with a hazardous event that is unlikely but possible to occur in the life of the system, subsystem, or component
- Unlikely but possible to occur in the life of an item; unlikely but can be expected to occur in fleet/inventory

E. Improbable

- P(incident) ≤ 1E-9 per operating hour
- Classification associated with a hazardous event that is so unlikely to occur that it can be assumed it will not be experienced in the life of the system, subsystem, or component
- Very unlikely; it can be assumed occurrence may not be experienced; unlikely to occur, but possible in fleet/inventory
- The E (Improbable) category is not interpreted as zero probability, thus, zero risk. It includes all items that are judged to have a low or extremely low probability of occurrence. There is no zero-probability category included in the ranking matrix.

Each hazard is rated for risk (Severity-Probability) as I-E, II-E, etc., in Table 2. Where the information was available (especially in cases where the risk may change for QMB as compared with O-PTC), probability ratings (A–E) have been included in the table. Since the risk assessment ratings for O-PTC were not available, they are not shown in the table.

4 Results of Safety Analysis

Overall, the results of the safety analysis presented in Table 2 indicate that, for comparable hazards between O-PTC and QMB, the residual risks will be lower with QMB operations supported by OSC, if proposed mitigations are implemented. For hazards that change with the introduction of QMB operations, the residual risks will be acceptable if proposed fail-safe implementation of safety-critical functions in the office segment, onboard segment, optional Vital Rear-of-Train Location (VRTL) segment, and optional advanced broken rail detection system and mitigations are deployed. The analysis presented herein shows that the OSC performs diverse checking of the result of every safety-critical PTC office function as part of a "Diversity and Self-Checking" SAC. This means that every safety-critical office function will be performed in a fail-safe manner with the proposed QMB (and FMB) office architecture.

This safety analysis is a preliminary draft that will require further update by any railroad choosing to implement the QMB (and eventually FMB) system supported by the OSC.

In this safety analysis, hazards are categorized into two different groups. Table 1 describes what each group includes and summarizes the main outcomes of the safety analysis contained in Table 2.

Table 1. Summary Results of the OSC Safety Analysis

Group	Description	Main Outcome of the Safety Analysis
PTCEA Overlaps Another Train's PTCEA	The most fundamental safety principle of QMB is the issuance of non-overlapping PTCEAs and the violation of this principle would lead to hazardous operations. Errors that can create this type of hazard could originate from the functions in the office. Hazard IDs from 1 to 5 in Table 2 are related to PTCEA handling and are part of this group.	The risks associated with these types of hazards can be mitigated to an acceptable level (I-E) by implementing the OSC to validate safety-critical office functions to make them fail-safe, as described in Table 2. For non-equipped trains, additional mitigation is also proposed to mitigate risks
O-PTC PTC-BOS-related Functions	This hazard is related to O-PTC office functions that convey safety-critical information to trains, such as: issuing track bulletins and handling PTC track data. Hazard ID 6 in Table 2 is part of this group.	Risk is reduced by implementing OSC to validate the safety-critical information in messages that the office conveys to trains, as described in Table 2.

Table 2. Hazard Risk Assessment Results

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
1	**PTCEA Overlaps Another Train's PTCEA**														
1.1-b	Overlapping PTCEAs are issued to trains	Incorrect handling of PTCEAs by Office.	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe. 2) Onboard segment, besides the fail-safe implementation of PTCEAs, receives WSMs with field status and applies the most restrictive of the two.	Office Segment/ Onboard Segment	1) OSC shall only insert RIC CRC for a PTCEA that does not overlap another PTCEA 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1051 messages when these are filled in with valid data (i.e., not filled with zeroes), which validates safety critical messages like PTCEAs in QMB.	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	Initial PTCEA	5.5.2.a-2 5.5.2.d-1	2.4.e-2 2.4.e-3 2.4.e-4	N/A	N/A
											PTCEA Extension	5.5.2.e-1		N/A	N/A
											PTCEA Modification	5.5.3.a-1		N/A	N/A
											Exclusive Bidirectional Authorities	5.5.7.1.a-1	2.9.a-2 2.9.a-3 2.9.a-4	N/A	N/A
1.1-b.1	Train receives a PTCEA that overlaps a protected section of track	Incorrect handling of PTCEAs by Office.	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe. 2) Onboard, segment besides the fail-safe implementation of PTCEAs, receives WSMs with field status and applies the most restrictive of the two.	Office Segment/ Onboard Segment	1) OSC shall only insert RIC CRC for a PTCEA that does not overlap another PTCEA 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1051 messages when these are filled in with valid data (i.e., not filled with zeroes), which validates safety critical messages like PTCEAs in QMB.	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	Initial PTCEA	5.5.2.a-2 5.5.2.d-1	2.4.e-2 2.4.e-3 2.4.e-4	N/A	N/A
											PTCEA Extension	5.5.2.e-1		N/A	N/A
											PTCEA Modification	5.5.3.a-1 5.12.b-1		N/A	N/A
											Exclusive Bidirectional Authorities	5.5.7.1.a-1	2.9.a-2 2.9.a-3 2.9.a-4	N/A	N/A
1.5	Train Operates with outdated PTCEA	Incorrect handling of PTCEAs by Office or Comms System, which causes the train to receive an outdated PTCEA (PTCEA that has already been voided or replaced by a newer PTCEA)	Collision (train-to-train, train-to-roadway worker, train-to-equipment)	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe. 2) Receiving and enforcing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe.	Office Segment/ Onboard Segment	1) OSC shall validate that every PTCEA that is issued is triggered by a valid process (train entering QMB territory or new train in QMB territory) before inserting the RIC CRC. 2) Onboard segment shall implement fail-safe mechanism to identify and discard duplicate PTCEAs (probably based on sequence number).	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	Initial PTCEA	5.5.2.a-2 5.5.2.d-1	2.4.e-2 2.4.e-3 2.4.e-4 2.9.a-2 2.9.a-3 2.9.a-4 2.10.a-2 2.10.a-3 2.10.a-4	New onboard segment requirement - the onboard segment shall verify that the PTCEA Id or sequence number is unique, to identify/reject previously voided/canceled PTCEAs	N/A
							1) OSC shall validate that every PTCEA that is issued is triggered by a valid process (PTCEA being extended because of CAD request or PTCEA rollup of the leading train) before inserting the RIC CRC.				PTCEA Extension	5.5.2.e-1		Same as above	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
							2) Onboard segment shall implement fail-safe mechanism to identify and discard duplicate PTCEAs received after having been previously voided/canceled (probably based on sequence number).								
							1) OSC shall validate that every PTCEA that is issued is triggered by a valid process (PTCEA being modified by CAD request) before inserting the RIC CRC. 2) Onboard segment shall implement fail-safe mechanism to identify and discard duplicate PTCEAs received after having been previously voided/canceled (probably based on sequence number).				PTCEA Modification	5.5.3.a-1 5.12.b-1		Same as above	N/A
							1) OSC shall validate that every PTCEA that is issued is triggered by a valid process (new exclusive work authority request from CAD) before inserting the RIC CRC. 2) Onboard segment shall implement fail-safe mechanism to identify and discard duplicate PTCEAs received after having been previously voided/canceled (probably based on sequence number).				Exclusive Bidirectional Authorities	5.5.7.1.a-1	2.9.a-2 2.9.a-3 2.9.a-4	Same as above	N/A
1.6	Train receives PTCEA that was created for another train	Incorrect handling of PTCEAs by the Office, which causes the system to send the PTCEA of one train to a different train	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe 2) PTCEA Messages to include error detection on destination addresses to protect against address corruption during communications. 3) Onboard segment to be able to identify some situations of PTCEAs incorrectly	Office Segment	1) OSC shall validate that every PTCEA recipient matches the recipient of the process that triggered it (train entering QMB territory or new train in QMB territory) before inserting the RIC CRC. 2) Messages shall include error detection on destination addresses to protect against address corruption during communications (already done in PTC). 3) OSC shall validate the transformation from train ID to loco ID in the PTCEA messages before inserting RIC CRC. 4) Existing O-PTC onboard SW functionality that verifies the	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	Initial PTCEA	5.5.2.a-2 5.5.2.d-1	2.4.e-2 2.4.e-3 2.4.e-4 2.9.a-2 2.9.a-3 2.9.a-4 2.10.a-2 2.10.a-3 2.10.a-4	N/A	N/A
											PTCEA Extension	5.5.2.e-1		N/A	N/A
											PTCEA Modification	5.5.3.a-1 5.12.b-1		N/A	N/A
											Exclusive Bidirectional Authorities	5.5.7.1.a-1	2.9.a-2 2.9.a-3 2.9.a-4	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
					assigned to train, if practical		RIC CRC of 1051 messages when these are filled in with valid data (i.e., not filled with zeroes), which validates safety critical messages like PTCEAs in QMB.								
1.7-b	Incorrect PTCEA conveyed to non-communicating train.	CAD system fails and displays incorrect PTCEA instructions to dispatcher.	Collision (train-to-train, train-to-roadway worker, train-to-equipment)	I	1) Implement interface between MB Office and voice radio system so that the office conveys a voice message with the PTCEA directly to train crew (after passing the safety check).	Office Segment and Operations / Support Personnel	1) Interface between the Office and voice radio system shall be implemented so that the office conveys a voice message with the PTCEA directly to train crew after passing the safety check.	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).		N/A	N/A	N/A	N/A
1.7-d	Incorrect PTCEA conveyed to non-communicating train.	Moving Block Office system fails and send incorrect PTCEA instructions to dispatcher.	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe. 2) PTCEAs for NENC trains to be sent to CAD or for verbal conveyance to train crews could be checked by QMB Office safety server before being sent.	Office Segment and Operations / Support Personnel	1) PTCEAs shall be validated by the OSC even for NENC trains before passing it to the delivery system, e.g., CAD.	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	PTCEA Issuance, Exclusive Bidirectional Authority, Joint Bidirectional Authority	5.5.2.a.2 5.5.2.d.1 5.10.b-1	2.4.e-2 2.4.e-3 2.4.e-4 2.9.a-2 2.9.a-3 2.9.a-4 2.10.a-2 2.10.a-3 2.10.a-4	N/A	N/A
1.7-c	The crew of a non-communicating / non-enforcing train incorrectly operates with incorrect limits of a PTCEA transmitted by the Dispatcher (like in voice authority)	The crew of a non-communicating / non-enforcing train incorrectly interprets/records the PTCEA transmitted by the Dispatcher (like in voice authority)	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Keep existing operational procedure rules that require, for example, train engineers to readback. 2) For NENC trains, there needs to be an absolute block established ahead of the train per 49 CFR 236.1029 (b)(5): "Where the PTC system is the exclusive method of delivering mandatory directives, an absolute block must be established in advance of the train as soon as safe and practicable, and the train shall not exceed restricted speed until	Office Segment and Operations / Support Personnel	1) Keep operational procedure rules that require train engineers to readback (as done today). 2) OSC shall identify a train as non-communicating and shall validate that PTCEAs for a non-communicating train to comply with an absolute block established ahead of the train per 49 CFR 236.1029 (b) (5): "Where the PTC system is the exclusive method of delivering mandatory directives, an absolute block must be established in advance of the train as soon as safe and practicable, and the train shall not exceed restricted speed until the absolute block in advance of the train is established." QMB shall leverage the nature of PTCEAs as	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	PTCEA Issuance	5.5.2.i-1 5.10.b-1	N/A	N/A	N/A
											Train starting trip or receiving initial PTCEA	5.5.2.i-1 5.10.b-1	N/A	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
					the absolute block in advance of the train is established." Note: A PTCEA is a form of absolute block since it has absolute limits		absolute blocks in ways that will be determined.								
1.8	Train receives a PTCEA including a portion of track for which a track bulletin has been issued, and the train has not received that track bulletin	Multiple causes: 1) Office does not send the track bulletin to the train; 2) Track Bulletin message is not delivered to train 3) Track Bulletin message is delivered to incorrect train	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins	I	1) Issuing bulletins is a safety-critical function that needs to be implemented fail-safe. 2) Implement mechanism that verifies that a train has received the track bulletins that contain tracks within the authority limits being issued to that train.	Office Segment	1) OSC shall validate the information in a track bulletin and insert RIC CRC only when the information is correct 2) OSC shall not insert RIC CRC to a PTCEA containing tracks affected by a track bulletin, if OSC has not received a corresponding track bulletin ACK message from the recipient train of the PTCEA 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1051 messages when these are filled in with valid data (i.e., not filled with zeroes), which validates safety critical messages like PTCEAs in QMB.	The assessment is described in the QMB Safety Analysis included in (Kindt, 2021).	The residual probability is specified in the QMB Safety Analysis included in (Kindt, 2021).	The residual risk is specified in the QMB Safety Analysis included in (Kindt, 2021).	PTCEA Issuance	N/A	2.4.e-2 2.4.e-3 2.4.e-4	N/A	N/A
2	Rolling Up PTCEAs														
2.1a	A train's PTCEA includes a section of track that was incorrectly released by another train	1) Incorrect handling of the PTCEA rollup by the Office, which frees tracks not yet released by a train	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Issuing non-overlapping PTCEAs is a safety-critical function that needs to be implemented fail-safe. 2) PTCEA rollup is a safety-critical function that needs to be implemented in a fail-safe manner	Office Segment	1) OSC shall validate a PTCEA rollup information before updating the list of active PTCEAs. If the information is correct, the PTCEA is updated and tracks are properly released, otherwise, the original PTCEA remains active, hence avoiding an incorrect release of tracks.	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be	Improbable (E) with the implementation of OSC, which makes MB Office functions, that process PTCEA rollups, fail-safe	Acceptable with Review (AC/WR) if OSC makes MB Office functions that process PTCEA rollups, fail-safe, based on the Severity-Probability categorization of I-E	Rolling up PTCEAs	5.5.4.i-1 5.5.4.j-1 5.5.4.k-1	2.5.a-1 2.5.a-2 2.5.a-3	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Romt(s)	OscSg Romt(s)	Onbd Romt(s)	Wayside Romt(s)
								implemented in the MBO with OSC to prevent issuance of overlapping PTCEAs.							
3	Following moves														
3.6-ba	A following train receives a PTCEA incorrectly specifying that the leading train has its rear-end in a fail-safe way.	1) MB Office incorrectly informs a following train that its leading train has rolled up its PTCEA with active VRTL.	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) MB Office functions that handle PTCEA roll-ups and following moves need to be implemented fail-safe.	Office Segment	1) OSC shall identify a train as leading and another as following when they fulfill the requirements of following move. 2) OSC shall validate the extension of a PTCEA of a following train in following move operation, verifying that the VRTL field indication in the PTCEA rollup message sent by the leading train matches the VRTL field indication in the PTCEA extension message being sent to the following train.	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent the Office incorrectly informing a following train that its leading train has rolled up its PTCEA with active VRTL.	Improbable (E) with the implementation of OSC, which makes MB Office functions, that inform a following train that its leading train has rolled up its PTCEA with active VRTL, fail-safe	Acceptable with Review (AC/WR) if OSC makes MB Office functions that inform a following train that its leading train has rolled up its PTCEA with active VRTL, fail-safe, based on the Severity-Probability categorization of I-E	PTCEA Issuance, Following Moves	5.5.5.d-1	2.4.e-2 2.4.e-3 2.4.e-4 2.6.a-1 2.6.b-1	N/A	N/A
4	**Exclusive Bidirectional Authorities**														
4.1a	Train receives a PTCEA extension based on the incorrect bidirectional PTCEA void	1) Office incorrectly processes PTCEA void of train with exclusive	Collision (train-to-train, train-to-roadway worker, train-to-	I	1) Office function that handles Exclusive Bidirectional Authorities needs to be implemented fail-safe	Office Segment	1) OSC shall not archive an active exclusive bidirectional PTCEA until it verifies the train has cleared the section of tracks within the PTCEA limits. Until then, it will keep the original PTCEA in the list of active	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for	Improbable (E) with the implementation of OSC, which makes MB Office	Acceptable with Review (AC/WR) if OSC makes MB Office functions that process the	Exclusive Bidirectional Authorities	5.5.7.1.a-1 5.5.7.1.a-2 MB Office shall not process PTCEA void of a train	2.9.a-5	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
	of another train (with VRTL)	work authority	equipment).				PTCEAs, hence that section of track protected.	QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent incorrectly processing PTCEA void of train with exclusive work authority	functions, that process the PTCEA void of a train with a Exclusive Bidirectiona l Authority (with active VRTL), fail-safe	PTCEA void of a train with an Exclusive Bidirectional Authority (with active VRTL), fail-safe, based on the Severity-Probability categorization of I-E		with an exclusive bidirectional authority			
4.2a	Train receives a PTCEA extension based on the incorrect bidirectional PTCEA void of another train (without VRTL)	1) Office incorrectly processes PTCEA void of train with exclusive work authority	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Office function that handles Exclusive Bidirectional Authorities needs to be implemented fail-safe	Office Segment	1) In signaled territory, WSMs inform a train that a block is occupied, and restricted speed is enforced. In non-signaled territory, absolute block train spacing is necessary. 2) OSC shall not archive an active exclusive bidirectional PTCEA until it verifies the train has cleared the section of tracks within the PTCEA limits. Until then, it will keep the original PTCEA in the list of active PTCEAs, hence that section of track protected.	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent incorrectly	Improbable (E) with the implementation of OSC, which makes MB Office functions, that process a PTCEA void of a train with a Exclusive Bidirectiona l Authority (without active VRTL), fail-safe	Acceptable with Review (AC/WR) if OSC makes MB Office functions that process a PTCEA void of a train with a Exclusive Bidirectional Authority (without active VRTL), fail-safe, based on the Severity-Probability categorization of I-E	Exclusive Bidirectional Authorities	5.5.7.1.a-1 5.5.7.1.a-2	2.9.a-5	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Romt(s)	OscSg Romt(s)	Onbd Romt(s)	Wayside Romt(s)
								processing PTCEA void of train with exclusive work authority							
4.3a	Train receives a PTCEA extension which limits fall inside the PTCEA limits of a train with an exclusive bidirectional authority	1) Office incorrectly processes PTCEA rollup of train with exclusive work authority	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Office function that handles Exclusive Work Authorities needs to be implemented fail-safe	Office Segment	1) OSC shall not validate the PTCEA rollup of a bidirectional authority. It will keep the original PTCEA in the list of active PTCEAs, hence that section of track protected	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent incorrectly processing PTCEA rollup of train with exclusive work authority	Improbable (E) with the implementation of OSC, which makes MB Office functions, that process a PTCEA rollup of a train with a Exclusive Bidirectional Authority, fail-safe	Acceptable with Review (AC/WR) if OSC which makes MB Office functions that process a PTCEA rollup of a train with a Exclusive Bidirectional Authority, fail-safe, based on the Severity-Probability categorization of I-E	Exclusive Bidirectional Authorities	5.5.7.1.a-1 5.5.7.1.a-2 MB Office shall not process PTCEA rollups of a train with a bidirectional authority	2.9.a-5	N/A	N/A
4.4a	Train receives PTCEA update removing RSR within the limits of the Exclusive Bidirectional PTCEA	1) Office incorrectly processes PTCEA rollup of train with unidirectional authority before it leaves the Exclusive Bidirectional PTCEA limits	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Office function that handles Exclusive Work Authorities needs to be implemented fail-safe	Office Segment	1) OSC shall not insert RIC CRC into a PTCEA update message removing RSR restriction within an Exclusive Bidirectional PTCEA limits before confirming there are no other active PTCEAs within those limits	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is	Improbable (E) with the implementation of OSC, which makes MB Office functions, that processes PTCEA rollup of train with unidirectiona	Acceptable with Review (AC/WR) if OSC makes MB Office functions, that processes PTCEA rollup of train with unidirectional authority, fail-safe, based on the Severity-Probability	Exclusive Bidirectional Authorities	5.5.7.1.b-1 5.5.7.1.c-1	2.9.b-1 2.9.b-2	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
								critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent incorrectly processing PTCEA rollup of train with unidirectional authority before it leaves the Exclusive Bidirectional PTCEA limits	1 authority, fail-safe	categorization of I-E					
5	Switching Operations														
5.1a	Train receives a PTCEA extension into the limits of a train performing switching operations	1) Office incorrectly processes PTCEA rollup of train with switching limits	Collision (train-to-train, train-to-roadway worker, train-to-equipment).	I	1) Office function that handles PTCEA rollups needs to be implemented fail-safe	Office Segment	1) OSC shall not validate the PTCEA rollup of a train inside the switching limits. It will keep the original PTCEA in the list of active PTCEAs, hence that section of track protected 2) Onboard segment shall not roll up its PTCEA while on switching operations	Higher level of safety integrity (such as can be achieved with the mitigation proposed) is needed for QMB as compared with Overlay PTC (O-PTC). QMB is not an overlay system – QMB safety is critically dependent upon there being no overlap in PTCEAs. Safety-critical functions must be implemented in the MBO with OSC to prevent incorrectly processing the PTCEA rollup	Improbable (E) with the implementation of OSC, which makes MB Office functions, that process PTCEA rollups, fail-safe	Acceptable with Review (AC/WR) if OSC makes MB Office functions, that process PTCEA rollups, fail-safe, based on the Severity-Probability categorization of I-E	Switching Operations	5.5.8.a-1 5.5.8.b-1 5.5.8.c-1 MB Office shall not process PTCEA rollups of a train with switching limits	2.11.a-1	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Romt(s)	OscSg Romt(s)	Onbd Romt(s)	Wayside Romt(s)
								of a train in Switching limits							
6	BOS-related Functions														
6.1	Train receives incorrect information in track bulletin	Multiple causes: 1) PTC-BOS processes incorrectly the track bulletin information received from CAD, 2) communicatio n system issues corrupt the message	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins	I	1) Issuing track bulletins is a safety-critical function that needs to be implemented fail-safe.	Office Segment	1) OSC shall validate the information in the Track Bulletin message prepared by PTC-BOS and insert RIC CRC only when the information is correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1041 messages when these are filled in with valid data (i.e., not filled with zeroes).	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	Improbable (E) with the implementati on of OSC, which makes O-PTC Office, that convey Track Bulletin messages, fail-safe	Acceptable with Review (AC/WR) if OSC makes O-PTC Office, that convey Track Bulletin messages, fail-safe, based on the Severity-Probability categorization of I-E	Track Bulletin Issuance	5.8.a-1	2.14.a-2 2.14.a-3 2.14.a-4	5.8.a-2 5.8.b-1 5.8.b-2 5.8.b-3	
6.2	Train does not receive a Track Bulletin message	The Track Bulletin message is not sent to all trains due to an error of the PTC-BOS or the communicati on system.	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins	I	1) Issuing track bulletins is a safety-critical function that needs to be implemented fail-safe.	Office Segment/ Onboard Segment	1) OSC shall not provide RIC to a PTCEA containing track affected by the track bulletin when the office has not received the bulletin ACK message from the recipient train	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	Improbable (E) with the implementa tion of OSC, which makes O-PTC Office functions, that convey Track Bulletin messages and MB Office functions that issue PTCEAs, fail-safe	Acceptable with Review (AC/WR) if OSC makes O-PTC Office functions, that convey Track Bulletin messages and MB Office functions that issue PTCEAs, fail-safe, based on the Severity-Probability categorization of I-E	PTCEA Issuance	N/A	2.4.e-2 2.4.e-3 2.4.e-4	N/A	N/A
6.3	Track Bulletin message is sent to incorrect train	BOS inserts incorrect recipient address into the Track	1) Collision (train-to-train, train-to-	I	1) Issuing track bulletins is a safety-critical function that needs to be implemented fail-safe.	Office Segment	1) OSC shall validate the recipient of the track bulletin and the transformation from train ID to loco ID performed by the PTC PTC-BOS. It provides	Higher level of safety integrity can be achieved using the Moving	Improbable (E) with the implementa tion of OSC, which	Acceptable with Review (AC/WR) if OSC makes O-PTC	Track bulletin Issuance	N/A	2.14.a-2 2.14.a-3	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Romt(s)	OscSg Romt(s)	Onbd Romt(s)	Wayside Romt(s)
		Bulletin message	roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins				RIC CRC only when the information is correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1041 messages when these are filled in with valid data (i.e., not filled with zeroes).	Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	makes O-PTC Office functions, that convey Track Bulletin messages, fail-safe	Office, that convey Track Bulletin messages, fail-safe, based on the Severity-Probability categorization of I-E			2.14.a-4		
6.4	Train operates with corrupted track data	BOS mishandles track database information while constructing the message	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins	I	1) Track database information is safety critical and needs to be handled in a fail-safe manner	Office Segment	1) OSC shall store its own copy of the database with a fail-safe design and whenever the PTC-BOS sends a PTC track database or any message that contains information related to PTC track database, the OSC can safely validate its contents and only add the RIC CRC when those are correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of safety critical messages when these are filled in with valid data (i.e., not filled with zeroes).	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	Improbable (E) with the implementation of OSC, which makes O-PTC and MB Office functions that handle track data in messages that include the RIC CRC field, fail-safe	Acceptable with Review (AC/WR) if OSC makes O-PTC and MB Office functions that handle track data in messages that include the RIC CRC field, fail-safe, based on the Severity-Probability categorization of I-E	PTC Track Data Management	N/A	2.15.a-1 2.15.a-2 2.15.b-1 2.15.c-1 2.15.d-1 2.15.d-2 2.15.d-3 2.15.e-1 2.15.e-2	N/A	N/A
6.5	Train operates with incorrect mandatory directives	BOS mishandles information while constructing the Current Dataset List message	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins.	I	1) PTC Authorities and bulletins are safety-critical information that needs to be handled in a fail-safe manner	Office Segment	1) OSC shall validate the information contained in the message (authorities, bulletins, track data version) and that PTC territory is in the territory list of the recipient train. OSC inserts the RIC CRC when the information is correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1022 messages when these are filled in with	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This	Improbable (E) with the implementation of OSC, which makes O-PTC Office functions, that convey Current Dataset List	Acceptable with Review (AC/WR) if OSC makes O-PTC Office functions, that convey Current Dataset List messages, fail-safe, based on the	Current Dataset List	N/A	2.16.c-1 2.16.c-2 2.16.c-3	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
			2) Train operating at excess speed which can cause derailment in case of Form A bulletins				valid data (i.e., not filled with zeroes).	can be done in O-PTC and QMB territories.	messages, fail-safe	Severity-Probability categorization of I-E					
6.6	Train operates with incorrect mandatory directives	BOS inserts incorrect recipient address in the Current Dataset List message while constructing it	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment in case of Form A bulletins	I	1) PTC mandatory directives are safety-critical information that needs to be handled in a fail-safe manner	Office Segment	1) OSC shall validate the recipient of the Current Dataset List Message is the same train that sent the (2022) request message. OSC inserts the RIC CRC when the information is correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1022 messages when these are filled in with valid data (i.e., not filled with zeroes).	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	Improbable (E) with the implementation of OSC, which makes O-PTC Office functions, that convey Current Dataset List messages, fail-safe	Acceptable with Review (AC/WR) if OSC makes O-PTC Office functions, that convey Current Dataset List messages, fail-safe, based on the Severity-Probability categorization of I-E	Current Dataset List	N/A	2.16.c-1 2.16.c-2 2.16.c-3	N/A	N/A
6.7	Train operates with incorrect mandatory directives	BOS mishandles information while constructing the Office Segment Poll message	1) Collision (train-to-train, train-to-roadway worker, train-to-equipment) in case of Form B bulletins. 2) Train operating at excess speed which can cause derailment	I	1) PTC mandatory directives and track data are safety-critical information that needs to be handled in a fail-safe manner	Office Segment	1) OSC shall validate the information contained in the message and that PTC territory is in the territory list of the recipient train. OSC inserts the RIC CRC when the information is correct 2) Existing O-PTC onboard SW functionality that verifies the RIC CRC of 1021 messages when these are filled in with valid data (i.e., not filled with zeroes).	Higher level of safety integrity can be achieved using the Moving Block Office's OSC to perform the mitigation proposed with the O-PTC Office. This can be done in O-PTC and QMB territories.	Improbable (E) with the implementation of OSC, which makes O-PTC Office functions, that convey PTC Segment Poll messages, fail-safe	Acceptable with Review (AC/WR) if OSC makes O-PTC Office functions, that convey PTC Segment Poll messages, fail-safe, based on the Severity-Probability categorization of I-E	PTC Office Segment Poll	N/A	2.16.b-1 2.16.b-2 2.16.b-3	N/A	N/A

Hazard ID	Hazard Description	Hazard Cause	Potential Hazard Effect	Severity Category	Potential Mitigation(s)	Subsystem or Person	Existing PTC or Proposed QMB Hazard Mitigation(s)	Assessment	Residual Probability	Residual Risk	Condition	MbOfcSg Rqmt(s)	OscSg Rqmt(s)	Onbd Rqmt(s)	Wayside Rqmt(s)
			in case of Form A bulletins												

5 References

[1] U.S. Government Publishing Office, Title 49 Code of Federal Regulations Part 236, Appendix C to Part 236– Safety Assurance Criteria and Processes, Washington, DC: Federal Railroad Administration.

[2] Report: Institute of Electrical and Electronics Engineers, Inc., "IEEE Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control," IEEE, 2000.

[3] Association of American Railroads, "PTC Office-Locomotive Segment - ICD Standard S-9361 V2.0," *Manual of Standards and Recommended Practices*, Washington, DC: AAR, 2014.

[4] Kindt J. (in press). Quasi-Moving Block Positive Train Control, Federal Railroad Administration.

Abbreviations and Acronyms

Acronym	Definition
ABS	Automatic Block Signaling
ACK	Acknowledgement message
AJBA	Advanced Joint Bidirectional Authority
BOS	Back Office Server
CAD	Computer-Aided Dispatch
CAD-MA	CAD Movement Authority
CIXL	Centralized Interlocking
CIXL-F	Centralized Interlocking Field Segment
CIXL-O	Centralized Interlocking Office Segment
ConOps	Concept of Operations
CP	Control Point
CRC	Cyclic Redundant Check
CTC	Centralized Traffic Control
EMP	Edge Message Protocol
EO-PTC	Enhanced Overlay PTC
EOT	End-of-Train
FMEA	Failure Modes and Effects Analysis
FMB	Full Moving Block
FRA	Federal Railroad Administration
GCOR	General Code of Operating Rules
GPS	Global Positioning System
HMAC	Hash-based Message Authentication Code
HMI	Human-Machine Interface
HRA	Hazard Risk Assessment
HRCTC	Higher Reliability and Capacity Train Control
HRI	Hazard Risk Index
ICD	Interface Control Document

Acronym	Definition
ICD	Interface Control Document
ITC	Interoperable Train Control
ITCM	Interoperable Train Control Messaging
IXL	Field Interlocking
MA	Movement Authority
MAS	Maximum Authorized Speed
MBO	Moving Block Office
MSRP	Manual of Standards and Recommended Practices
MTTHE	Mean-Time-To-Hazardous-Event
NACK	Negative Acknowledgement Message
NENC	Non-Enforcing Non-Communicating
O&SHA	Operation and Support Hazard Analysis
OC	Object Controller
O-PTC	Overlay PTC
O/S	On Sheet
OSC	Office Safety Checker
PHA	Preliminary Hazard Analysis
PTC	Positive Train Control
PTCDP	PTC Development Plan
PTCEA	PTC Exclusive Authority
QMB	Quasi-Moving Block
RAM	Reliability, Availability, and Maintainability
RIC	Redundant Integrity Check
RSIA ‘08	Rail Safety Improvement Act of 2008
RSR	Restricted Speed Restriction
SAC	Safety Assurance Concepts
SCAC	Standard Alpha Carrier Code
SegRS	Segment Requirements Specification
SHA	System Hazard Analysis

Acronym	Definition
TAG	Technical Advisory Group
TBC	To Be Configured
TBD	To Be Determined
TME	Train, Men, or Equipment
TTCI	Transportation Technology Center, Inc.
TWC	Track Warrant Control
VRTL	Vital Rear of Train Location
WIU	Wayside Interface Unit
WSM	Wayside Status Message
WSRS	Wayside Status Relay Service
XML	Extensible Markup Language