U.S. Department of Transportation
Federal Railroad Administration

RESEARCH RESULTS
FRA OFFICE OF RESEARCH, DEVELOPMENT & TECHNOLOGY

RR 23-04 | **May** 2023

OFFICE SAFETY CHECKER FOR MOVING BLOCK TRAIN CONTROL SYSTEMS

SUMMARY

As part of a research project sponsored by the Federal Railroad Administration (FRA) between June 2020 and May 2022, 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.

Figure 1 presents the MBO architecture with the OSC component. The proposed architecture is advantageous from the perspective that it reduces the vitality to a minimum number of functions when used in conjunction with a fail-safe onboard system that verifies the Cyclic Redundancy Checks (CRCs) and Hash-Based Message Authentication Codes (HMACs) applied by diverse office systems. Further, the OSC is contained in a single environment that decouples it from functions that implement business rules (e.g., the Computer-Aided Dispatch (CAD) Movement Authority (MA) parsing or CAD interface functions) that do not necessarily need a fail-safe implementation.

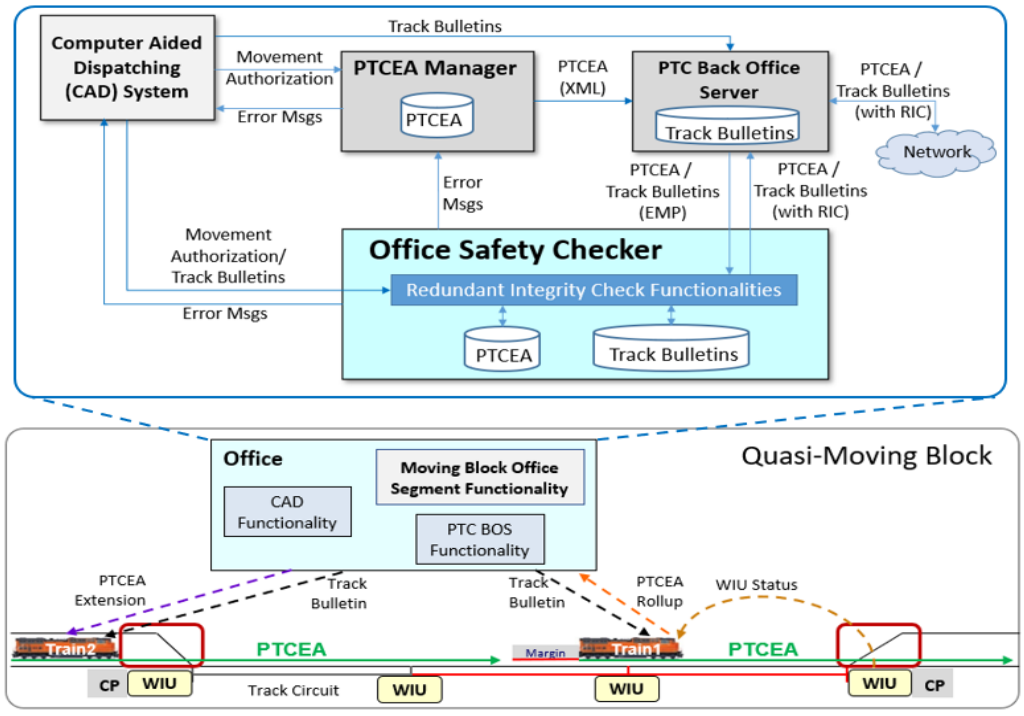

Figure 1. MBO Office and OSC Architecture

The proposed concept follows the Safety Assurance Concept (SAC) of "Diversity and Self-Checking" for the verification of vital functions. The team developed the Segment Requirements Specification (SegRS) based on this SAC, leveraging the QMB system and segment requirements and including the necessary modifications and additions required for OSC implementation.

Researchers also performed the following OSC Safety Analyses:

- MBO hazards associated with the safety-critical functions
- PTC-BOS hazards associated with functions that handle messages with safety-critical information sent from the office to trains
- The risks associated with these types of hazards

From these analyses, the team concluded that risks can be mitigated to an acceptable level by implementing the OSC to safely validate the office functions considered safety-critical for QMB and Full Moving Block (FMB) operations.

BACKGROUND

New methods of train control that have the potential to enhance railway safety, reliability, and operational performance while leveraging PTC technology have been identified and researched. The current form of PTC technology, referred to here as Overlay PTC (O-PTC), has the potential to evolve into a method of train control that supports these needs, and the team identified three potential new modes of train control: Enhanced Overlay PTC (EO-PTC), QMB, and FMB.

Both the QMB and FMB concepts use an exclusive, non-overlapping movement authority known as a PTC Exclusive Authority (PTCEA) to grant movement authority to each train in the territory. The MBO functions manage the creation of PTCEA messages, the electronically delivered artifacts that train crews depend on for safe train operation. The data within these PTCEA messages is safety-critical and requires validation for the safety of rail network operations.

As a spin-off of the QMB project, the current project was created to develop the systems engineering specifications for an OSC component that validates MBO functions considered safety-critical.

OBJECTIVES

The objective of this project was to produce OSC functionality system engineering documentation that each railroad can use to pursue further development. This documentation includes:

- OSC Concept of Operations (ConOps)
- OSC SegRS Specification
- OSC Safety Analyses

METHODS

During this project, the team created OSC documentation that railroads can use in future development. The creation of these documents is discussed below.

OSC ConOps

This document includes the OSC architecture, features, functions, failure modes, and a high-level implementation plan.

From a functional standpoint, the OSC validates the group of MBO and PTC-BOS functions considered safety-critical. The OSC does not introduce operational functionality beyond that provided by the MBO and PTC-BOS systems. However, the OSC does define the safety requirements and system design characteristics that must be pursued to allow those functions to be implemented in a fail-safe manner.

OSC SegRS Specification

The team developed the OSC SegRS that defines the functions the OSC must perform to validate the safety-critical functions of the MBO and the PTC-BOS.

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

OSC Safety Analyses

The team performed OSC safety analyses limited to the hazards related to MBO functions that are different in QMB (including OSC) as compared with O-PTC.

The safety analyses 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 on the O-PTC system.

Safety analyses were performed from three standard perspectives culminating in a Hazard Risk Assessment (HRA). These three perspectives are:

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

RESULTS

The proposed concept adopts the "Diversity and Self-Checking" SAC defined in IEEE1483-2000 [1] and in Appendix C of 49CFR236 Subpart I [2] as the SAC for the OSC, since it accommodates the use of a safety checker. This SAC is used to ensure that failures are detected and the train is automatically placed in a safe state when those failures occur.

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

In the proposed concept, the OSC checks that every safety-critical office function is performed correctly. The OSC uses the Redundant Integrity Check (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. The RIC CRC is checkable for errors by the onboard segment receiving the message.

The train's onboard segment verifies that the message contents are consistent with the RIC CRC in that message, similar to how it handles 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 an error found during the validation computation), the onboard segment discards the message and sends a notification to the MBO.

CONCLUSIONS

The proposed OSC does not add operational functionality to the MBO and O-PTC systems; rather, it defines safety requirements and system design characteristics that enable safety-critical functions to be implemented in a fail-safe manner. The QMB/FMB safety-critical functions included in the OSC design are primarily those related to the issuance and validation of PTCEAs. The team applied the Diversity and Self-Checking SAC defined in IEEE1483-2000 [1] and Appendix C of 49CFR236 Subpart I [2] collectively to the PTCEA Manager, PTC-BOS, and OSC segments working together with the onboard segment so 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.

The OSC safety checking functionalities related to the PTC-BOS (e.g., safety checking of track bulletins, office segment poll, and current dataset list messages) are optional in the sense that they can be implemented in 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 these safety checking functionalities.

The OSC functionality works in conjunction with the PTCEA Manager so that the MBO can perform QMB and/or FMB office functionality in a fail-safe manner. Therefore, the implementation of the OSC must occur simultaneously with the implementation of the rest of the MBO components.

The OSC safety analyses include the identification of potential hazards associated with MBO and PTC-BOS safety-critical functions, the risks associated with these hazards, and how these risks can be eliminated or mitigated. Based on these analyses, the team concluded that risks can be mitigated to an acceptable level with OSC implementation.

REFERENCES

[1] 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.

[2] 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.

[3] Association of American Railroads (2014). PTC Office-Locomotive Segment - ICD Standard S-9361 V3.0. *Manual of Standards and Recommended Practices*, Washington, DC: AAR, 2014.

ACKNOWLEDGEMENTS

TTCI would like to acknowledge members of the Train Control, Communications, and Operations (TCCO) committee for their contributions to the development of the OSC project.

CONTACT

Jared Withers
Federal Railroad Administration
Office of Research and Development
1200 New Jersey Avenue, SE
Washington, DC 20590
(202) 493-6362
jared.withers@dot.gov

Moyah Wilson
Office of Acquisition Services
U.S. Department of Transportation
Federal Railroad Administration
(202) 493-6222
moyah.wilson@dot.gov

KEYWORDS

Quasi-Moving Block (QMB), Full-Moving Block (FMB), Positive Train Control (PTC)

CONTRACT NUMBER

DTFR53-11-D-00008L