This paper discusses the necessity and challenges for suppliers of mass transportation signaling systems to design extra safety features on top of modern signaling systems’ operational safety properties to support safe integration and migration (i.e. cut-over transition) during field implementation. Suppliers traditionally focus on designing a system to be safe for delivering advanced operation functions and leave the field engineering safety to be managed through procedures. However, with increases of complexity associated with various field integration and migration scenarios as required by customers or enforced by field engineering environments, the stepwise integration and migration of a signaling system itself can raise new hazards, which cannot easily be managed by procedures. There are additional safety challenges in a re-signaling project during migration from the existing legacy system. Thus, this paper suggests that the system’s design should have designed-in safety mechanisms to ensure the safety of not only the future operation, but also the field integration and migration. Specifically, it highlights the significance of identifying hazard conditions associated with interactions between the many controllers and devices at each step of system integration and migrations. It then discusses how to manage challenges of designing safety logic to mitigate these field migration hazards.

Introduction

Advanced signaling systems maximally automate train operations to make urban rail transit systems offer high reliability, punctuality, and operational efficiency. In large cities, urban rail transit systems are considered the main approach to resolve traffic difficulties and living environment problems. As the world’s population is constantly on the rise, more people are living in cities, which results in:

- Extension of cities in size, requiring constructions of new metro lines and extending tracks of existing ones. This offers green field projects for signaling in new tracks;
- Increase of population density, requiring upgrades of existing lines with advanced signaling systems to improve capacity and efficiency. This situation offers brown field projects to replace or overlay existing signaling systems with more advanced systems.

Almost all signaling projects have very demanding construction schedules and complicated field conditions, which raise significant challenges of how to ensure system integration safety. System integration is a complicated process to compose the system capability by assembling and installing many components and tuning them through testing so that they work together as designed to deliver expected functions and safety features for revenue operation. A more advanced signaling system has more components and functions, thus it needs more time in
installation, integration, and commissioning. Also, the railway working environment presents various hazards. Signaling system suppliers and integrators endeavor to find an effective field integration approach on each project to manage schedule and safety risks.

In the signaling domain, Communications-Based Train Control (CBTC) signaling systems are designed based on the most advanced technology from computers and communication networks, which offer not only advanced signaling functions but also the flexibility for incremental implementation and integration. A CBTC system delivers Automatic Train Supervision (ATS) functions for routing trains according to predefined schedules and Automatic Train Operation (ATO) functions for controlling train movement. This can effectively reduce human operation delays and separation distance between trains to improve service capacity. More importantly, comparing against traditional signaling systems, a CBTC system significantly enhances the train operational safety through real-time Automatic Train Protection (ATP) functions, which prevent hazards from human errors, internal failures, or unexpected events resulting in accidents. Because of these mentioned advantages, CBTC systems are very popular in both new mass transit system projects and re-signaling projects.

However, implementing a CBTC system in the real field itself is much more complicated comparing to a traditional interlocking signaling system, leading to great safety challenges. At first, there are many pieces of equipment and devices to be installed in different geographic locations along tracks and each of them must be validated against its specifications fitting in various CBTC functions. Second, the CBTC system itself has a large number of functions delivered by interactions between many controllers, other electronics, and electrical devices. Due to civil construction progress limitations, the field installation, integration, and validation can only be done incrementally when commissioning a system. Third, a re-signaling project has additional complexity from cut-over mechanisms or mixed operation scenarios between the CBTC system and the existing legacy system. Re-signaling projects which upgrade existing service lines raise significant challenges in CBTC integration logic designs. Switching back and forth between legacy systems (for continuing normal operation during service time) and the new CBTC integration (during engineering time for field testing) is naturally prone to hazards.

This paper discusses safety challenges associated with field integration of a CBTC system, and proposes to design safety features in the CBTC system integration logic to ensure field engineering safety. A CBTC system is normally integrated in the manner of track zone by track zone, and thus how to prevent a testing train unintentionally going out of the integration zone needs technical design support. Especially, CBTC field integration and testing on a re-signaling project needs special safety features to ensure safety of cut-over transitions between two systems. This paper proposes an approach to designing safety features into CBTC systems to mitigate their field engineering hazards. These features need systematic efforts to identify and design them as built-in safety logic of the system to support integration safety management. Thus, the approach to developing these safety features should parallel and complement the normal system safety program. The analysis in the proposed approach can enhance traditional system safety engineering programs to achieve designed-in safety logic and safety features to ensure the safety of not only future operation, but also system field integration and migration.
Safety Concerns in CBTC Signaling System Integration and Migration

CBTC system suppliers naturally focus on designing a system to be safe for delivering advanced train operation functions in order to survive as a business in the signaling domain. As enforced by common standards (American Railway Engineering and Maintenance-of-Way Association, 2011; European Committee for Electrotechnical Standardization, 2003; International Electrotechnical Commission, 2002; US Department of Defense, 1993, 2012), a supplier defines and executes a systematic safety engineering program to develop the safety case of a final system to achieve safety certification for service operation. However, there is no standard to obligate suppliers to design safety features in signaling systems to facilitate field integration safety. It is quite common that field engineering safety is managed by procedures. In reality, integration of CBTC systems shows insufficiency of using procedures to mitigate most field hazards due to:

- Increased complexity of CBTC systems, which makes integration steps often have mutual dependency. The partially integrated configuration may show some unexpected behavior against previously defined procedures.
- Various field integration and migration scenarios as enforced by customers, which make procedures very different between projects. Especially, procedures developed for a resignaling project can be very complicated for managing transitions between the existing legacy system and a configuration of the partially integrated CBTC system. Insufficiency of procedures results in hazards not only in the CBTC integration, but also in the legacy system operation.

Thus, it is necessary to design certain safety features in CBTC systems to facilitate field integration safety management.

Referring to the simplified CBTC system model illustrated in Figure 1, a CBTC system has several kinds of subsystems as follows:

- **Automatic Train Supervision (ATS)**, which consists of a number of controllers located in the control center and interlocking stations. The ATS provides scheduling and automatic routing of trains for continuous operation, and offers user interfaces for operators to command the CBTC system for special operational maneuvers. It commands Zone Controllers to implement trains’ routes and control trains’ movement authority, as well as to implement operator commands for controlling trackside devices. ATS controllers collect wayside and trackside equipment statuses including train locations to display to operators. The ATS communicates with train onboard controllers to supervise and collect train operation statuses for operators. In a real system, the number of both central and local ATS subsystems often exceeds 10.

- **Zone Controller (ZC)**. The ZC installed for each geographic signaling zone controls and monitors wayside devices, protects each train in the zone, sets up train routes and enforces interlocking, and provides train movement authority for safe train separation from any obstruction. The ZC tracks train locations and status information through communications with train onboard controllers, and detects non-communicating trains based on track block occupancy status. The ZC also monitors trackside devices in a real-time manner, and responds to any failure in these devices by informing trains to react appropriately. In a real system, the number of ZC subsystems exceeds 10.

- **Vehicle Onboard Controller (VOBC)**. The VOBC on a train offers ATO and ATP functions according to the movement authority issued by a ZC. ATP functions in the VOBC ensure the
train to be operated within the current movement authority. The VOBC detects and mitigates failures and unexpected events from train-lines and driver errors. The VOBC determines the train location in real-time based on detected transponders, the internal track map, switch positions from ZC communications, and data from speed sensors and accelerometers. The VOBC reports train position and status to the ATS and the ZC. In a real system, the number of VOBC subsystems can exceed 100.

- Data Communication System (DCS). The DCS is the backbone of the CBTC system to enable all controllers to communicate with each other to deliver the expected CBTC functions. In CBTC designs, the safety and security mechanisms are important built-in properties for safe operations. For reliable communications between CBTC controllers, redundant backbone networks and mobile radio communication networks are used to give the CBTC system flexibility of integration and feasibility of extension in the future.

Based on our experience of developing CBTC systems on multiple projects (Shi, 2012, 2013), safety of CBTC system integration faces significant challenges to manage the following hazards:

- Hazard 1: High speed train movement intruding into a trackside work zone. During CBTC field integration, people often need to work on the trackside for various reasons, and a train moving into the work area at a high speed is a hazard. It is expected to have some effective technical measures to protect a work zone by enforcing trains be driven manually at low speed in the work zone.

- Hazard 2: Train movement on a moving or unlocked switch. This situation is a hazard resulting in train derailment. During integration, this hazard is raised very often due to using an interlocking route without completing the route validation.

- Hazard 3: Unintended train movement going out of integration testing area. Especially, a train used for the CBTC integration testing may unexpectedly go out of the integration possession area, possibly moving to the installation area where workers are on the track.

- Hazard 4: Unexpected interactions between a certified service zone controller and a zone controller under testing. This situation can raise hazards because the zone controller under
testing may not correctly track train traversal from its territory to the revenue operation zone resulting in train detection and protection errors in the service ZC. The consequences of this hazard can be train collisions.

A re-signaling project not only has the hazards mentioned in the previous paragraph, but also adds hazards from switching back and forth between the existing legacy signaling system and the partially integrated CBTC system. Because the legacy signaling system’s service operation must not be interrupted, the CBTC field integration can only be performed at night in a 4 or 5 hour time window. Thus, switching between the existing signaling system and the partially integrated CBTC system is daily routine work, which needs time to power up or down the CBTC devices and also to confirm both systems’ working condition on each transition. All these make the CBTC integration time window even smaller, which increase the risk to project schedules. Thus, it is important to design special safety mechanisms that can confidently let CBTC controllers stay in the powered up state (i.e. a shadow mode) during legacy system service operation hours. Because these CBTC controllers have not been validated to be safe, they may intrude on the legacy system. The following conditions are hazards:

- **Hazard 5**: CBTC controllers under integration intruding into legacy system service operation may result in hazards in the legacy signaling train separation functions leading to collisions.
- **Hazard 6**: Legacy system intruding into the CBTC integration. Possible hazardous conditions can be created due to conflicting switch lock control resulting in a CBTC test train derailment.

Field integration of a signaling system has many chances to result in the above mentioned hazards during field integration. Hazard 1 and Hazard 2 are noteworthy hazardous conditions for almost all signaling projects. If a project strongly demands early revenue service, the new signaling system often has to be opened incrementally in a track zone by track zone manner. In such a situation, Hazard 3 and Hazard 4 are notable safety concerns. Re-signaling projects are notorious difficulties and have the extra distinguished hazards: Hazard 5 and Hazard 6.

**Systematic Approach to Designing Safety Features for Integration and Migration**

As discussed in the previous section, the safe integration logic with sufficient safety features for ensuring field integration of a system should be systematically designed into the system. These safety features are expected to simplify field procedures to reduce the risk of hazards associated with system integration. The effectiveness of these features in the integration logic is strongly related to the integration approach on a project. An effective integration approach lays the foundation for defining and designing practical safety features into the system to ensure safety of field integration and to meet the customer’s integration requirements. Also, these safety features should be part of the future CBTC system safety properties and must be developed based on reviewing previous projects’ integration experience, analyzing the current projects’ integration plans, and predicting future CBTC integration scenarios. Thus, these safety features not only facilitate integration hazard management on a project but will also be used in the final system for managing special operation needs and maintenance scenarios.

In essence, the systematic approach for developing these safety features as part of the system integration logic follows the generic safety engineering process:
• Performing hazard analysis, which includes identifying hazards in possible engineering activities in various integration scenarios and environment conditions associated with the system integration and migration approach. The outputs of hazard analyses result in enhancing the integration and migration plan and defining corresponding technical hazard mitigations to be specified as safety requirements;
• Designing safety features to meet these safety requirements and implementing them in hardware and software, as well as defining the necessary instructions for using these features;
• Validating and demonstrating the safety features in both in-house and field testing to ensure their correctness in supporting field system integration and testing.

For identifying all possible contributors in the system integration and testing phase to the hazards mentioned in the previous section, the hazard analyses are performed from the following aspects for identifying practical and effective safety features:
• Hazardous conditions from external factors, which may exist in customer’s requirements and field engineering constraints for system integration and commissioning. Mitigations to these conditions are imported inputs for defining safety features.
• Possible incomplete validation of interlocking routes resulting in train traversal to an unlocked switch during integration testing and subsequent derailment. In reality, integration testing often needs trains going through a switch that has not completed validation of its locking logic on all related routes. Thus, identifying all possible contributors to the switch hazards and their corresponding mitigations is very important for field integration testing.
• Unexpected behavior or conditions in controllers’ interactions in a partially integrated system configuration. The corresponding analysis needs to cover possible combinations of controllers and devices as a field configuration during system integration and testing. This analysis leads to enhancing existing safety mechanisms or adding new safety features.
• Defects in the integration strategy, which may lead to a hazardous sequence of integration. With consideration of possible errors from intensive human involvement during integration, the analysis leads to consolidating the integration strategy and adding safety features for ensuring the safety of transitions from one step to the next during integration and testing.

Based on the attributes of the CBTC system configuration and previous field integration experience, including lessons learned from previous projects, the effective integration strategy is the incremental integration to be carried out in control zone by control zone as follows:
• Control Zone internal integration: Under the condition that the zone under integration is isolated from its neighboring zones, all devices and controllers in this control zone are integrated against their responsibilities with the exemption of interfaces with the neighboring zones.
• Control Zones’ interface integration: When two neighboring zones have their internal integration completed, the interface integration between them can be started and subsequently completed for delivering CBTC train functions.

Thus, the hazard analyses can be divided into two categories: hazards associated with the zone internal integration and hazards associated with zone interfaces for integrating any two zones.

Safety features for supporting CBTC system integration and testing must be effective in design and correct in implementation. They are derived from the hazard mitigations mentioned above with consideration of reusing existing CBTC safety properties. All safety features are designed
in software and hardware to meet vitality. On a project, due to customization driven by guideway data and environmental constraints, they must be verified and validated through in-house and field testing to ensure their correctness before use.

**Expected Safety Features in CBTC Designs to Prevent Field Integration Hazards**

From our practice on multiple CBTC projects and knowledge of possible challenges in integration of future CBTC systems, we expect to design the generic integration logic and safety features in the CBTC product. They can be customized for managing various integration and migration scenarios requested by customers or limited by field environment conditions. By applying the systematic approach as described in the previous section, we have analyzed the current projects’ integration plans and our CBTC integration experience on previous projects, as well as possible field engineering scenarios predicted for future projects. This systematic analysis effort leads us to determine the generic integration strategy, the integration logic and safety features as designed-in properties of the CBTC product. The design of these features offers flexibility to customize these safety features on a project for ensuring safety of the system integration and migration. This approach has been demonstrated as effective on the current projects’ field integration and migration scenarios.

The safety features are designed at first to facilitate safety management of integrating all devices in a zone (i.e. a zone internal integration) and re-signaling project cut-over migrations within a zone, and then to provide safety mechanisms for integrating any two zones for testing train traversal through the zone boundary. There are different integration and migration scenarios in a zone internal integration, which are chosen by either the customer or the integrator on a project. These safety features offer the flexibility to support these scenarios by defining the integration and migration steps, which satisfy the customer’s expectation and make the cost effective tradeoffs for the integrator. Also considering possible human operator errors in enabling and disabling safety features during the system integration and migration, the safety features are designed with diverse logic to overlap each other to mitigate a hazard condition. As a result of our effort, the following safety features are designed in the CBTC product:

- **Safety features for a zone internal integration and testing to use:**
  - Work Zone protection, which prohibits a train in an automatic mode from entering into the zone and enforces a low speed for a manual train. This feature mitigates Hazard 1.
  - Automatic Train Mode Inhibit Zone, which can require a train travel through the zone in a manual train operation mode other than an automatic mode. This feature can be used to further mitigate Hazard 1.
  - Operator Switch lock, which enables the operator to lock a switch in a specific position to prevent it moving to the other position by a route calling and it also only permits a manual train route to go through it, which enforce a testing train to be driven in manually at a quite low speed. This is designed to mitigate Hazard 2.
  - Operator Switch Blocking, which enables the operator to block any switch movement command and prevent any movement authority to be granted to an approaching train to go to the blocked switch. This is designed to mitigate Hazard 2 and Hazard 3 in the case of the switch being used to limit the testing area.
  - Lock a signal on Red, which locks a signal in Red even if its permissive condition is true. This feature is intended to prevent a manually driven train from moving into a work
zone, and can be used to enforce the ends of the testing area. This is designed to mitigate Hazard 3 for any train regardless its mode to stop before the signal, and also Hazard 4 by locking the boundary entry signal to Red of a service zone to prevent any train entry.

- Close Tracks, which prevents a CBTC train movement to or within these tracks. This feature can be used for managing emergency situations encountered during integration testing. This feature can also be used further to mitigate Hazard 3 by closing the end tracks of a testing area and Hazard 4 by closing the testing zone boundary tracks.
- Temporary Speed Restriction (or Go Slow Zone), which can require a CBTC controlled train to travel at the intended low speed in a specific track zone during integration. This feature can be used for mitigating Hazard 1 by setting a lower speed on top of a work zone protection and Hazard 3 by setting zero speed at the end tracks of a testing area.

Safety features for supporting integration between zones to prevent Hazard 2 and other train operation hazards on a zone boundary, which include:

- The safety futures mentioned for zone internal integration to manage the border area by setting Temporary Speed and Automatic Train Mode Inhibit Zone.
- The following are existing CBTC safety logic, which can be validated first and then used further to facilitate the hazard management during integration of two control zones:
  - Crossing border route interlocking: All routes crossing a ZC-ZC border have interlocking logic, and the authorization of each route in the hand-over zone (i.e. departure zone) has the pre-condition that the take-over zone (i.e. destination zone) has already locked and authorized the portion of the route in its territory. This ensures safety of train traversal across the zone boundary.
  - Crossing border route cancellation interlocking: If the operator cancels a crossing border route, the take-over zone can cancel the portion of the route if only if the hand-over zone completes its cancellation. This ensures that the train approaching the route or already on the route has stopped before the route is cancelled.

Safety features for separating two control zones to prohibit trains’ traversal: This is designed as further mitigation of Hazard 4 for the case that one zone is already in service operation while the other zone is still under integration testing. These features are explained as follows:

- Closing border, which closes a specific border of a control zone with its neighboring zone to prevent any train going to the neighboring zone and also to prohibit a train entry from the neighboring zone into its territory. This feature can be used in the service zone controller with safety confidence.
- Prohibit collaboration with another zone controller, which can be used to inform a revenue operation zone controller not to make train detection and tracking decisions based on any information from the neighboring zone controller under integration and testing. This prevents any testing zone’s error in tracking a train crossing the border from causing failures of detecting a non-communicating train entry in the revenue zone.

Safety features for migrating Hazard 5 and Hazard 6, which are designed for managing cut-over between the legacy signaling system and the CBTC system under integration:

- Cut-over box in a control zone, which is a vital hardware mechanism to switch trackside device controls exclusively between the CBTC system and the legacy signaling system. This cut-over box switching status can be used to trigger the CBTC zone controller to go to a shadow mode, in which no outputs from it can reach physical devices, and vice versa for the legacy system. It is also important that the zone controller in shadow mode should not generate a movement authority to be used for any train. To ensure this,
related trains need to know the ZC mode and have cut-over mechanisms as well for safety of the legacy system operation.

- Cut-over switch for a train, which is a vital switch circuit that can switch the train to be controlled either by the controller of the legacy system or by the VOBC of the CBTC system exclusively. When a train is controlled by the legacy system controller, the VOBC outputs are cut off (i.e. no capability to command the train system). The VOBC will inform the ZC that it is in the cut off state (also known as the shadow mode). If the ZC is in control, the train can only be routed by using the fixed block logic.

The safety features mentioned above are designed in the CBTC product based on a generic CBTC system integration strategy (in the manner of control zone by control zone). On a project, the integration and cut-over plan will be made by following the generic integration strategy to define effective integration steps by using the built-in safety features to satisfy the customer integration requirements and specific environment constraints.

Based on our practice on the integration and migration of several CBTC systems, the designed-in safety features have demonstrated their effectiveness in mitigating hazards associated with the system integration and migration, which significantly reduced the field integration schedule risk on these projects. For a specific project, the CBTC product including these safety features is customized by the specific guideway data (such as tracks, blocks, platforms, and zones) and trackside physical devices (such as switches, signals, and platform doors). The system integration as planned is performed in steps for zone internal integration or the integration between zones. These safety features must be validated as early as possible in the first integration zone, and can then be used in subsequent integration activities. For each remaining zone, these safety features only need to test their correspondence with the trackside devices and guideway data in the zone to achieve safety and efficiency of integration and testing in the zone. Internal integration of a control zone consists of the following steps:

1. Pre- and Post- Installation Check Out tests of all devices, which confirm that each device is qualified and connections between these devices are correct as designed.
2. Element functional tests, which verify functionality of each trackside device as specified and qualify trains for the CBTC VOBC to control.
3. Integrating CBTC wayside core safety functions, which verify switch movement and locking logic, route setting and interlocking. Especially, the designed safety features for supporting integration must be validated through field testing.
4. Testing ATP functions with protection provided by the safety features. Testing train interfaces first and then the positioning function. Subsequently, integrate the rest of ATP functions incrementally.
5. Testing ATO functions, which now have protection provided by ATP functions.

The integration of two zones which have their internal integration done is not complicated in our practice because safety features have been tested and can now be used in this integration. The crossing border route interlocking and the crossing border route cancellation interlocking need to be tested first and then train traversal boundary logic can be tested.

For a project with re-signaling or multiple stage opening attributes, the cut-over box in a control zone and the cut-over switch for a train must be tested before other integration testing. This can support the CBTC equipment to stay in a powered on state while trains operate in the legacy
signaling system. After validation of the zone separation safety features (closing border and prohibiting collaboration with another zone controller) is done, they can be used to manage safety of the boundary between a revenue zone and a zone under integration.

**Conclusion**

Integration of a large scale safety critical system such as a CBTC system itself has various hazards that need mitigations from safety features to be designed into the system. This paper presented a systematic approach for developing these expected safety features as an important part of the system integration logic. Based on our experience on a number of CBTC projects, the safety features designed in the CBTC system in this approach have demonstrated their effectiveness to ensure safety of the CBTC systems’ integration and testing, as well as safety of switching back and forth between a legacy and CBTC system on a re-signaling project.

The safety features developed in the systematic approach discussed in this paper can be used not only to facilitate safety management during the system integration and testing, but also to offer safety measures for the final system with respect to failure management and corrective maintenance.

**References**


