Risk Analysis of a CBTC Signaling System

João Batista Camargo Jr.¹, Jorge Rady de Almeida Jr.¹, Paulo Sérgio Cugnasca¹

¹ Escola Politécnica da Universidade de São Paulo, São Paulo-SP, Brazil

Abstract

The aim of this paper is to present a preliminary work of a Risk Analysis of the CBTC – Communication Based Train Control – Signaling System used in Subway Transport Systems. A CBTC is an automatic continuous train control system utilizing high-resolution train location determination independent of track circuits. It has high supervision and control capacity and bidirectional train-to-wayside data communications. This paper presents a preliminary work of CBTC Risk Analysis, highlighting some relevant characteristics related to its main components: checking balise, radio communications network, CBTC wayside equipment and train borne CBTC equipment. A HAZOP technique is applied over some of these components. The necessity of knowledge about this kind of system, considering its probable use in the São Paulo Subway, can contribute for the determination of relevant safety parameters.

1. Introduction

This paper presents a preliminary work of Risk Analysis of a CBTC – Communication Based Train Control – Signaling System of a Subway Transport System. A CBTC is an automatic continuous train control system using high-resolution train location determination independent of track circuits. It has high supervision and control capacity and bidirectional train-to-wayside data communications.

The Risk Analysis process is divided into four phases: System Description, including its Interfaces; Hazard Analysis; Residual Risk Qualification and Evaluation; and Operational Experience Evaluation. Preliminary Hazard Analysis, System Hazard Analysis, Subsystem Hazard Analysis, Operation and Support Hazard Analysis and Final Hazard Analysis compose the Hazard Analysis Phase. At this way, it is presented in this paper a Preliminary Hazard Analysis of a CBTC system highlighting some relevant characteristics related to their mains components: checking balise, train borne CBTC equipment, radio communications network and CBTC wayside equipment.

The necessity of knowledge about this kind of system, considering its probable use in the São Paulo Subway, can contribute for the determination of relevant safety parameters, since we have been worked as an Independent Safety Analysis Group for the São Paulo Metro Company.

2. Preliminary Hazard Analysis

The Preliminary Hazard Analysis involves [1]:

- determining what hazards might exist during operation;
- developing guidelines, specifications, and criteria to be followed;
- initiating actions for the control of particular hazards;
- identifying management and technical responsibilities for action and risk acceptance; and
- determining the magnitude and complexity of the safety problem.

In this paper, the first three aspects are considered. The first step is to identify the CBTC system, its boundaries and limits of resolution.
2.1. CBTC System Architecture

Figure 1 presents the CBTC System Architecture adopted in this paper.

The CBTC Wayside Equipment manages all trains in their zones (authority areas) and defines the movement authority limits for each train, as presented in Figure 2. This movement authority limit is periodically communicated to each train with other status data via the Radio Communication Network and, by the other hand, each train returns status information such as its position. The CBTC Wayside Equipment also receives information from the signals and switching machines, coming from the Track Equipment Controller. Each zone is divided into many virtual blocks which are sized to meet headway performance [2].

The Radio Communication Network shall provide continuous geographic coverage within CBTC territory and shall support train operation in tunnels and bidirectional data transfer.

The Train Borne CBTC Equipment is responsible for processing inputs/outputs for train control. The Train Borne CBTC Equipment controls high performance, service and emergency brake controls, door opening and closing, and regulates different operation modes, when permitted. The Train Borne CBTC Equipment communicates with the CBTC Wayside Equipments through the Radio Communications Network, and receives the position information of the checking balises [3].
2.2. CBTC Hazards

At least, a CBTC system shall address the following system hazards presented in Table 1, through the implementation of ATP – Automatic Train Protection functions [4]:

<table>
<thead>
<tr>
<th>Hazard</th>
<th>Ways of Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>train-to-train collisions</td>
<td>train separation assurance, rollback protection, parted consist protection and coupling and uncoupling of trains, route interlocking protection, and traffic direction reversed interlock</td>
</tr>
<tr>
<td>train-to-structure collisions</td>
<td>end-of-track protection and restricted route protection</td>
</tr>
<tr>
<td>train derailments</td>
<td>over speed protection, route interlock protection, and broken rail detection</td>
</tr>
<tr>
<td>crews and maintenance people</td>
<td>CBTC work zone protection functions</td>
</tr>
<tr>
<td>passengers associated with train movement with doors opened</td>
<td>interface between the Train Borne CBTC Equipment and the Train Door Subsystem to provide door opening control protection interlocks, zero speed detection, and departure interlocks.</td>
</tr>
</tbody>
</table>

Table 1: CBTC main hazards

2.3. General Guidelines

The general guidelines are based on standard IEEE-1474.1 [4].

A CBTC system design shall include capabilities to permit periodic verification of ATP, including verification of responses to interference on the Radio Communications Network.

The Radio Communications Network shall be sufficient to support all required ATP, ATO (Automatic Train Operation) and ATS (Automatic Train Service) functions and shall exhibit sufficiently low latency to support the defined performance requirements. Beside that, the Radio Communications Network shall include a protocol structure capable to assure minimum safety requirements.

The CBTC train location determination shall, safely and accurately, establish the location of both the train front and rear. The CBTC train location determination functions shall be self-initializing and shall automatically detect and establish the location of each CBTC train and recovery from CBTC equipment failures, without requiring manual input of train location or train length data.
The CBTC train speed determination function shall provide sufficient speed measurement resolution and accuracy to support the safety requirements. The CBTC shall compensate measurement inaccuracies effects on train location and speed determination. Specifically, if they are dependent upon wheel rotation, the CBTC system shall correct position errors induced by wheels slipping or sliding, and shall correct position errors caused by variation in wheel size due to wear, truing or replacement.

Safe train separation shall be provided between all trains operation in CBTC territory. The CBTC safe train separation function shall consist of the ATP profile calculation. The ATP profile shall be governed by a safe breaking model and shall ensure that under no circumstances, including failures, a train will exceed the movement authority limit.

The emergency brake rate considered shall be the minimum emergency brake rate available by a train, considering worst-case latent brake equipment failures modes.

A CBTC system shall ensure that under no circumstances, including failures, the train’s actual speed will exceed its safe speed, which shall be derived by considering the most restrictive conditions.

The rollback protection shall be a required ATP function for any CBTC system configuration.

End-of-track protection shall be incorporated in conjunction with over speed protection to prevent trains from reach dangerously the end-of-track, based on the safe breaking model.

Where separate vehicles can be coupled together, with two or more vehicles forming a train, a CBTC system shall have the detection capability and protection of isolated trains. A CBTC system shall also support operating requirements for coupling and uncoupling of trains, including length automatic updating within the CBTC system.

Zero speed detection shall be a required ATP function for any CBTC system configuration. Opened doors control protection interlock shall be another required ATP function.

The interlocks shall prevent a stationary train from moving, unless all train doors are properly closed and locked.

A CBTC system shall provide route interlocking functions equivalent to conventional interlocking practice, preventing trains collisions and derailments. The switching machines shall also be locked when the track section, containing the switching machine, is occupied by a train (detector locking).

In the event of a CBTC train location failure, route locking shall remain in effect until the train all the restrictive conditions are removed.

In the event of a switching machine indication loss, once a movement authority has been issued through an interlocking, a CBTC system shall pull back the movement authority to the entrance of the interlocking. If a train is already within a safe braking distance of the switching machine, the CBTC system shall initiate an immediate brake application.

Traffic direction reversal interlocks shall be a required ATP function for any CBTC system configuration.

A CBTC system shall not grant movement authorities to trains operation in out-of-service tracks or switching machines, and shall enforce restricted speeds on approach to and through defined maintenance zones.

A CBTC system might have interface with an auxiliary wayside system for broken rail detection purposes. In New York City Subway the decision was to incorporate single rail 60 Hz track circuits into its design to detect broken rail. Once it was determined that track circuits would be used for broken rail detection, it became clear that train circuits should also be used to provide the train detection function required by the Auxiliary Wayside System [5].
As specified by the authority with jurisdiction, a CBTC system shall include capabilities to prevent that a train enters in an unsafe route, due to mechanical, civil, electrical, or other predefined temporary or permanent route impediments.

2.4. Additional Recommendations for Particular Hazards Control

Considering the CBTC System architecture presented in Figure 1 and having in mind the CBTC hazards and general guidelines, previously exposed, a HAZOP – Hazard and Operability Study is applied over some of the most critical CBTC signals: maximum-speed (train) and position (input signals to Train Borne CBTC Equipment); position (train) (input signal to CBTC Wayside equipment).

HAZOP seeks to identify hazards by examining the possible failures of components and the interconnections between components. When a HAZOP is being carried out, there is normally some element of FMEA – Failures Modes and Effects Analysis – of the system components included within it [6].

As the design and operational conditions knowledge (including the systems environment) increases, four questions should repetitively be addressed:

- Does the design adequately address all previously identified hazards?
- Have any new hazard been introduced?
- Do the level of increased knowledge about system and its proposed or actual operation enable new hazards to be identified?
- What extra information can be gained about the potential causes and consequences of an earlier hazard identification?

HAZOP application to Programmable Electronic System – PES is a recent technique. Software is frequently overlooked during system analysis, but this is unacceptable when the software is in control of a potentially hazard operation. In such cases hazard analysis should be extended to completely cover the software and two questions should be addressed:

- If software operates in accordance with its specification, what is the potential effect on system hazard?
- If software operates incorrectly (deviates from its specification), what is the potential effect on system hazard?

Some aspects must be considered when the software has a critical role is the system:

- Software responds inadvertently to stimuli;
- Software fails to respond when required;
- Software responds out-of-sequence;
- Software responds in unplanned combination with other actions.

There are at least four potential impacts of software on each hazard [7]:

- Software may challenge the application safety systems: failure of the software to operate correctly has the potential for creating a hazardous condition that must be removed or mitigated by some other system;
- Software may be responsible for preventing a hazard from progressing to an incident;
- Software may be used to move the system from a hazardous state to a non-hazardous state;
- Software may be used to mitigate the consequences of an accident.
The identification of decisions is based on the use of predetermined “guide words”, each of which focuses attention on a particular type of possible deviation. The “guide words”, used in this analysis, are described by their interpretation for PES as follows:

**NO**: No data or control signal passed;

**MORE**: Data is passed at higher rate than intended, or more data is passed;

**LESS**: Data is passed at a lower rate than intended, or less data is passed;

**PART OF**: The data or control signals are incomplete;

**OTHER THAN**: The data or control signals are complete but incorrect;

**EARLY**: The signal arrives too early with reference to a correct time;

**LATE**: The signal arrives too late with reference to a correct time;

Each of the “Guide Words”, that were considered adequate for PES, will be applied in this CBTC Signaling System of a Subway Transport.

Tables 2 and 3 present the preliminary HAZOP analysis over Train Borne CBTC Equipment and CBTC Wayside Equipment. For instance, considering maximum-speed (train) signal, input to Train Borne CBTC Equipment, the guide word **NO** recommends that the train borne CBTC equipment shall have a time-window control of maximum-speed (train). In case of maximum-speed (train) time validity goes out of pre-defined time-window, the train borne CBTC equipment shall apply restrictions conditions to guarantee safe train separation. The others analysis are presented with details in Tables 2 and 3 and, when necessary, illustrated with Figure 3.

### 3. Conclusions

The standard IEEE Std 1474 says that a System Safety Program shall be instituted during CBTC system planning/design phase and shall continue throughout the system life cycle. The CBTC System Safety Program shall emphasize the accidents prevention by identifying and resolving hazards in a systematic manner, as the Risk Analysis process presented in this paper. As in New York Subway, it is highly recommended that exists a safety certification of the vital components of the CBTC system made by independents agencies. This paper presented a Preliminary Hazard Analysis of a CBTC System based on HAZOP – Hazard and Operability Analysis to PES – Programmable Electronic Systems. Through this technique some preliminary conceptual recommendations were obtained and highlighted.

### References


## Train Borne CBTC Equipment

<table>
<thead>
<tr>
<th>Signal</th>
<th>Guide Word</th>
<th>Particular Hazard</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>The maximum-speed (train) is not updated</td>
<td>The train borne CBTC equipment shall have a <strong>time-window</strong> control of maximum-speed (train). In case of maximum-speed (train) time validity goes out of pre-defined <strong>time-window</strong>, the train borne CBTC equipment shall apply restrictions conditions to guarantee safe train separation. (a)</td>
<td></td>
</tr>
<tr>
<td>MORE</td>
<td>The maximum-speed (train) is received at a higher rate than intended.</td>
<td>Same of (a)</td>
<td></td>
</tr>
<tr>
<td>LESS</td>
<td>The maximum-speed (train) is received at a lower rate than intended.</td>
<td>Same of (a)</td>
<td></td>
</tr>
<tr>
<td>PART OFF</td>
<td>The maximum-speed (train) received is incomplete.</td>
<td>The train borne CBTC equipment shall verify this failure through the protocol diagnostic and shall apply restrictions conditions to guarantee safe train separation. The Radio Communications Network shall include a protocol structure to support this aspect. (b)</td>
<td></td>
</tr>
<tr>
<td>OTHER THAN</td>
<td>The maximum-speed (train) received is complete but incorrect.</td>
<td>Same of (b)</td>
<td></td>
</tr>
<tr>
<td>NO</td>
<td>The position of a train is not updated by the information of the check balise.</td>
<td>The CBTC train location determination shall recovery from this failure, considering a “virtual bubble” representing the imprecise position of a train, as presented in Figure 3, to guarantee safe train separation. (c)</td>
<td></td>
</tr>
<tr>
<td>PART OF</td>
<td>The position received is incomplete.</td>
<td>Same of (c)</td>
<td></td>
</tr>
<tr>
<td>OTHER THAN</td>
<td>The position received is complete but incorrect.</td>
<td>Same of (c)</td>
<td></td>
</tr>
<tr>
<td>EARLY</td>
<td>The position arrives too early with reference to correct time.</td>
<td>The CBTC train location determination shall consider the difference between the position received from the check balise and the position calculated by the train borne CBTC equipment. If this difference is greater than a pre-defined value, in function of inherent imprecision of the CBTC system, the CBTC train location determination shall recovery from this failure, considering a “virtual bubble” representing the train position (Figure 3) to guarantee safe train separation. (d)</td>
<td></td>
</tr>
<tr>
<td>LATE</td>
<td>The position arrives too late with reference to correct time.</td>
<td>Same of (d)</td>
<td></td>
</tr>
</tbody>
</table>

Table 2: Preliminary HAZOP of train borne CBTC equipment.
The position (train) is not updated. The CBTC Wayside Equipment shall consider this failure to calculate the maximum speed of the all involved trains through the use of “virtual bubbles” to guarantee safe train separation.

The position (train) is received at a higher rate than intended. The CBTC Wayside Equipment shall verify this failure through the use of a “time-window”. In case of the time validity of position (train) goes out of this pre-defined “time-window”, the CBTC Wayside Equipment shall calculate the maximum speed of the all involved trains through the use of “virtual bubbles” to guarantee safe train separation. (a)

The position (train) is received at a lower rate than intended. Same of (a)

The position (train) received is incomplete. The CBTC Wayside Equipment shall verify this failure through the protocol diagnostic and consider it in the calculation of the maximum speed of the all involved trains using the concept of “virtual bubbles” to guarantee safe train separation. The Radio Communications Network shall include a protocol structure to support this aspect. (b)

The position (train) received is complete but incorrect. Same of (b)

Table 3: Preliminary HAZOP of CBTC wayside equipment.

Figure 3: Safe train separation considering the imprecision of trains location determination.