Modeling and security analysis of CBTC signal failure scenario based on ScOLA

Xiaotong An¹, Jinbai Zou²*, Zhukai Shen³, Shunyu Yao⁴

¹-⁴ Faculty of Railway Transportation, Shanghai Institute of Technology, Shanghai, 201418, China

*Corresponding author’s e-mail: zoujb@sit.edu.cn

Abstract. For the entire phase of the design, manufacture and operation of the Communication Base Train Control (Communication Base Train Control, CBTC) signal system, safety is the primary issue that needs to be considered. This article introduces ScOLA's modeling language, combined with the situation of the wireless loss fault of the vehicle-mounted signal equipment, and carries out a formal description and step-by-step simulation of the system. It further illustrates that the application of the ScOLA modeling language can perform the safety analysis of the CBTC signal system faster and more accurately.

1. Introduction

Traditional model-based security analysis methods cannot automatically generate security analysis from the system description model due to the complexity and difference of the system and model. This article will introduce a new method of system description, the extended language ScOLA of SDL (Issad et al., 2014)[1]. Using the ScOLA scenario modeling language can help system engineers formally define and verify the system starting from the informal and textual description of the system, and help synchronize the system and the security model. Based on the characteristics of the ScOLA modeling language, taking into account the characteristics of industry application diversity and safety, combined with the case of wireless loss failure scenarios of vehicle-mounted signal equipment, this paper demonstrates ScOLA's contribution to the safety analysis of CBTC signal system. In the methodology stage, this article will introduce them roughly and apply them to specific case studies.

2. The architecture of the CBTC signal system

The communication-based train operation control (CBTC) system is a block system technology used in the urban rail transit train automatic control system (ATC), which is parallel to the fixed block system controlled by the speed code and the quasi-mobile block system based on the target distance control. The latter two blocking systems are also applied in some domestic urban subway lines.

The CBTC system breaks through the limitations of track circuits and the shackles of fixed/quasi-mobile block. The basic features are:

(1) High-precision train positioning without relying on track circuits.

(2) The continuous vehicle-ground and ground-vehicle data communication network can transmit more control and status information than traditional systems.

(3) Trackside and on-board core processors process train status and control data, and can provide automatic train protection (ATP), automatic train driving (ATO) and automatic train monitoring (ATS) functions.
3. Scene-oriented rail transit system modeling language ScOLA

3.1. Background
Modeling is the most formal way for engineers to communicate, and its accuracy cannot be ignored. Formal models have been used to design and develop systems, or to analyze system safety and verification purposes, such as Method B, Simulink.

ScOLA is based on many concepts that include the system structure and its operating behavior, and is determined by the system architecture and its multiple views (functional view, structural view, and event-based view). This language allows engineers to define formal systems in a manner similar to natural language, solving problems such as lack of clarity of the system and the heterogeneity of methods and tools used in security analysis. The goal is to build a bridge between the people who design the system and verify the system. It is of great significance in ensuring that the system applying safety technology is correct, detailed and formal.

3.2. Functions and advantages
Bahr defines safety analysis as the application of engineering and management principles, standards and technologies to achieve acceptable accident risks at all stages of the entire system life cycle, under the constraints of operational effectiveness and applicability, time and cost. (Arnold et al., 1999) [2] (Yakymets et al., 2013)[3] proposed a model-based safety analysis (MBSA) method. Their goal is to introduce mathematical artifacts in which system and security engineers use the same system model. The goal of ScOLA is to make a complete and formal system model for safety analysis, and its safety analysis method is similar to fault propagation technology.

ScOLA not only incorporates safety considerations in the initial design, but also has the following advantages:

1) Automatically generate security analysis from the system description model
   Due to the complexity and difference of systems and models, even in some fields (such as aviation), the system engineer and the safety engineer must work separately to make the analysis go smoothly.

2) Avoid heterogeneity of methods and tools used in safety analysis
   Traditional model-based security analysis methods, their goal is to introduce mathematical tools. The rail transit system is characterized by a limited number of identified fault accidents, so safety analysis is mainly based on the study of the fault scenarios that lead to these accidents. These situations are bad behaviors that must be avoided or corrected in the system. At this time, the ambiguity of the system expression not only affects the understanding, it is also difficult to obtain the consistency and completeness of the analysis.

Figure 1. Overall architecture diagram of CBTC fully automatic operation signal system
(3) Contribute to the synchronization between the system and the security model
ScOLa solves the problem that security analysis cannot be automatically generated from the system description model due to the complexity and difference of the system and the model. Its view of security can start with language and form a technology that helps to synchronize the system and the security model.

4. Case study
The safety analysis technology of the rail transit industry is based on the analysis of potential scenarios. Because there are not many potential accidents in this field, deductive methods are used to improve the scenarios that lead to the accident before the failure is determined.

For fault detection in the CBTC signal system, especially possible faults in field components, it is very important to require harsh detection results. Therefore, when analyzing the performance of CBTC signal system, independent analysis of different parts can not reflect the overall performance. Because ensuring safe operation of Metro depends on the relationship between original parts of the site, it is necessary to ensure interoperability between different systems [4]. We will study the system model of its subsystems and check the diagnosability of each subsystem to show the overall diagnosability. In addition, the complex structure of electronic equipment and the interdependence between components and systems make it difficult to identify and analyze abnormal behavior [5]. For signal systems, this difficulty can be explained by a large number of undiscovered incidents or undefined faults recorded.

The hypothetical solution is that the on-board signal equipment has a wireless loss failure. After the failure occurs, the communication between the train and the ground is abnormal, resulting in the loss of train positioning, resulting in emergency braking [6]. It is assumed that the wireless cell has a long-term failure. If the communication failure continues, the train will take emergency braking. After the train stops, the driver must switch to RM (manual driving) mode to run to the next signal, and then switch to ITC (point train control) level. When the continuous communication is effective again, it can be switched back to the CTC (continuous train control) level [7]. Using the ScOLa modeling language, the operating behavior of the system will be realized individually or collaboratively through physical components. A scene can be decomposed into several sub-scenarios or a group of action behaviors, which can also be realized by physical components alone or in collaboration.

The case study is based on the following three steps:

- **Step 1:** Define the physical components related to the failure scenario. Analyze the signal system to understand the external factors (human factors or environmental factors) that may affect the system, what hazards exist in the system, and what may occur failures. In this scheme, the physical components are composed of trains, drivers, dispatchers, and tracksides.

- **Step 2:** Analyze the possible consequences after the failure occurs, as shown in Figure 3. Following ScOLa semantics and syntax, the scene is decomposed into a fact, that is, the scene represents a set of actions executed by one or two components after multiple optimizations. The fault-oriented action is converted into computer language, which is represented by the character f, as shown in Figure 4. f means that the model can be built by calling specific functions.

- **Step 3:** Perform security analysis for abnormal situations, which is represented by the character a. According to the different consequences, determine the system's response measures and strategies.

---

Figure 2. Schematic diagram of character description of fault-oriented action description
- $s_{0,1}$: The train signal system detects that the on-board signal equipment has a wireless loss fault
- $s_{0,2}$: The driver takes emergency braking
- $s_{0,3}$: The train shows the status of wireless loss failure. $s_{0,3}$ is the test scenario, followed by the sequence ($s_{0,4a}$, $s_{0,5a}$, $s_{0,6a}$, $s_{0,7a}$ and $s_{0,8a}$) or ($s_{0,4b}$, $s_{0,5b}$ and $s_{0,6b}$) or ($s_{0,4c}$, $s_{0,5c}$ and $s_{0,6c}$)
- $s_{0,4a}$: The train has been identified and stopped at the platform
- $s_{0,5a}$: The dispatcher orders to strengthen the station monitoring in the fault area
- $s_{0,6a}$: The dispatcher cooperates with the driver to open and close the train door
- $s_{0,7a}$: the train opens the door
- $s_{0,8a}$: The train will open the platform door to inform passengers
- $s_{0,4b}$: The train runs in the section
- $s_{0,5b}$: monitor the train interval in the faulty section, and strictly control the interval between trains above one axle counting section
- $s_{0,6b}$: The driver switches to RM mode and runs to the next signal machine.
- $s_{0,4c}$: The train leaves the wireless fault area
- $s_{0,5c}$: train positioning and receiving valid mobile authorization information from ZC
- $s_{0,6c}$: The train returns to the continuous communication AM/CM driving mode
- $s_{0,9}$: The driver controls the train to switch the ITC level
- $s_{0,10}$: The driver controls the train to switch the CTC level

The train signal system detects that the on-board signal equipment has a wireless loss failure, and the HMI displays the wireless cross (fault) icon

The on-board equipment takes emergency braking, and the HMI shows zero speed

The driver switches to RM mode and runs to the next signal machine

The driver can then switch the ITC level

After the driver waits for the continuous communication to be effective again, switch back to the CTC level

Figure 3. Failure flow chart of wireless loss

Figure 4. Graphical description of breakdown scenario breakdown
Security analysis of the program:
We consider the failure scenario s0,1.

- A1,1: When a failure causes a communication failure between the train and the ground, that is, when the OBCU (on-board control system) detects a communication failure with the ZC, the OBCU will not make any response within 3s. After 3s, the OBCU will order the ATO (Automatic Train Operation System) train to apply the service brake to slow the train.

- A1,2: OBCU will set the nearest location as the emergency brake point of the train, the next stop at the next station, the next chain signal, the communication loss stop (this stop will be based on the driver’s reaction time, the train’s speed Establish) waiting for a parking spot.

Regarding the possible failure modes of actions, there are the following two situations: component damage failure or interface failure of information transmission between components. The first case indicates that all subsequent operations implemented by that particular component will fail. In the second case, no matter which interface is damaged, the information will fail to be transmitted.

At this point of analysis, it is considered that the output of different safety-related actions and their respective failure modes, a1, 1, a1,2, have a priority relationship. This means that a failure of an action will cause it to be unable to proceed, and the entire program will fail.

Using previous information about actions and their interfaces, the following scenarios based on s0,1 can be determined:

1. a1,1 failed due to interface failure. If the ATS (Automatic Train Monitoring System) loses communication with the train, a warning will be sent to the ATS central operator/ATS local operator. The driver will continue to drive the train according to the display of the trackside signal.

2. a1,2 due to OBCU failure, ATO mode will not be authorized. Therefore, when the train stops, the operator switches the train mode to RMF (restricted forward manual driving mode) to move the train and re-establish position information.

This set of analysis methods not only allows analysts to clearly understand the specific operating principles of the system through the analysis process, and have a comprehensive understanding and grasp of failure scenarios, but also allows designers to consider the causes of hazards from a deep level, and design tests for hazards. Case, focus on testing the effectiveness of the fault handling design. Therefore, in the follow-up work, possible dangers can be avoided from the design layer and the implementation layer.

Engineers can choose to perform the following operations in the system safety analysis: insert one or more actions into the action flow chart triggered by the scenario to simulate the failure scenario. It has the feature of multiple tests and predicts possible failures. The advantage of this technique is that all dangerous behaviors can be found when considering the integrity of the system. By using known failure modes, action safety and functional scenarios, it is easy to place each action in a graphical description of its breakdown scenario. The characteristics of the ScOLa modeling language can focus the attention of safety analysis on optimizing the measures and solutions for troubleshooting. It can be executed independently from the real failure scenario, which is more convenient and efficient to use.

5. Conclusion
This paper uses a formal modeling language based on scenarios that describe the system architecture and behavior, and intends to analyze the wireless loss failures of on-vehicle signal equipment based on the perspective, explore the contribution of ScOLa to safety analysis, and avoid the limitations of safety analysis when the system fails. This feature greatly shortens the cycle of fault scenario modeling from design to safety analysis, and at the same time ensures the consistency of the implemented functions. ScOLa embodies more intelligent design ideas, and further enhances the ability of system engineers to intervene in safety analysis. By learning from the experience and lessons of scenario modeling safety analysis, it can make a significant contribution to avoiding similar failures.
ScOLA's safety analysis based on existing models can provide theoretical reference and technical support for the design, manufacturing and operation phases of the CBTC signal system, as well as failure safety. Developers can complete model construction by calling specific functions, and generate optimized netlists and files for the constructed modules, and export and generate corresponding security analysis files. The generated project file can be further edited to finally generate a safety analysis report based on failure scenario modeling. The exploration of ScOLA is still at a relatively early stage. I believe that in the near future, ScOLA will be put into use together with existing tools and languages.

Acknowledgments

This thesis was completed under the careful guidance of Teacher Zou, thanks to the strict requirements and careful guidance of the teacher. The brothers and sisters in the laboratory have provided enthusiastic help to my life and scientific research. I thank them for their company and make my scientific research road full of laughter. I would like to express my heartfelt gratitude to the tutor and fellow brothers!

REFERENCES

[1] Issad, M., Kloul, L., Rauzy, A. et al. Modeling the CBTC Railway System of Siemens with ScOLa. [M].Int. J. ITS Res. 16, 163–172 (2018).
[2] Arnold, A., G. Point, A. Griffault, & A. Rauzy (1999). The al tarica formalism for describing concurrent systems. Funda menta Informaticae 40(2), 109–124.
[3] Yakymets, N., H. Jaber, & A. Lanusse (2013). Model-based sys?tem engineering for fault tree generation and analysis. In MODELSWARD, pp. 210–214.
[4] Chen Mingsong, Bao Yongxiang, Sun Haiying, Miao Weikai, Chen Xiaohong, Zhou Tingliang. Trusted Construction of Train Control System Based on Communication: A Summary of Formal Methods [J]. Journal of Software, 2017, 28(05): 1183-1203.
[5] Feng Lijuan. Analysis of common failures of CBTC system on-board signal[J]. Modern Urban Rail Transit, 2011 (02): 39-42.
[6] Wang Hongbo, Gao Yu. Research on CBTC Train Control Level Switching Technology in Urban Rail Transit[J]. Modern Urban Rail Transit, 2017(02): 5-8.
[7] Xiao Yanbo. Discussion on the classification of urban rail transit CBTC system failure and its design countermeasures[J]. Modern Urban Rail Transit, 2011(03): 12-1