Design of system-level hot standby redundancy-based signal system

Yu Zhang$^{1,a}$, Xiaoyong Wang$^{2,3,b}$, Yi Yu$^{4,c}$, Pengzi Chu$^{1,4,d}$, Ye Xu$^{2,e}$

1 Telecom and Signal Branch, Shanghai Metro Maintenance Support Co., Ltd., Shanghai, 200235, China
2 CASCO Signal Co., Ltd., Shanghai, 200071, China
3 The Key Laboratory of Road and Traffic Engineering, Ministry of Education, Tongji University, Shanghai 201804, China
4 Maglev Transportation Engineering R&D Center, Tongji University, Shanghai, 201804, China

$^a$email: 13916577430@139.com, $^b$email: wangxiaoyong@tongji.edu.cn, $^c$email: 12164@tongji.edu.cn, $^d$email: cpz_myhk@163.com, $^e$email: xuye@casco.com.cn

Abstract. Focusing on the improvement of the availability for signal systems, a system-level heterogeneous hot standby redundancy-based signal system is discussed. The system includes a communication-based train control system (CBTC), a track circuit-based train control system (TBTC), and a switching unit. Under normal condition, the CBTC is connected to the communication system via the switching unit, and the function commands received by the train come from the CBTC. When the CBTC fails, the TBTC is connected to the communication system via the switching unit, and the function commands received by the train come from the TBTC. The switch between the CBTC and the TBTC is automatically executed by the system. Simulation results showed that the proposed design in this paper improved the availability of the signal system and reduced the impact of failures on operations.

1. Introduction
Urban rail transit has the characteristics of large passenger flow, high service frequency, and high criticality of safety and availability. Safety requirements are not only reflected in the safety operation of the urban rail transit system, but also in the guarantee of service quality [1]. With the automation of train operation control, the signal system has become a key subsystem in the system, playing the main role of train operation safety. Therefore, it is very important to ensure the availability of the signal system.

As a type of safety critical system, the signal system involves a large number of redundant technologies [2,3]. However, these contents are usually equipment-level. For example, the crucial control machine adopts a dual-machine mutual backup, double 2-vote-2, 3-vote-2, and even M-vote-N. However, the system level of the entire signal system does not have redundancy, only a backup degraded mode. For example, CTCS-3 (China Train Control System Level 3) lines may be equipped with CTCS-2 (China Train Control System Level 2), and CBTC lines may be equipped with intermittent fallback mode, but these cannot be called a system level hot standby redundant signal system. The equipment-
level redundancy method does not solve the impact of the equipment switching device failures on the signal system, and the degraded fallback mode will increase the switching time and reduce the function due to the degrading. Thus, the failures will eventually affect the normal operation, and the quality of a service can’t be guaranteed. Based on this, this paper proposes a system-level heterogeneous hot standby redundant signal system in view of the above-mentioned defects.

2. Literature review

The safety of train operation is directly related to the lives of passengers. With the deepening of the understanding on system safety, a way to improve system safety and availability has become a consensus, that is, to carry out pre-safety assessment and pre-security evaluation before system development, and then analyse and record potential hazards and failures as the main security problems to be solved in a research and development process [3]. Reliability refers to the ability of a product to complete a specified function within a specified time and under specified conditions [4]. The reliability of the signal system is related to the safety and quality of rail transit operations, and the dual methods of technology and management are needed to continuously improve system reliability. At the same time, people have higher and higher requirements on the punctuality and fulfilment rate of operations, and the signal system plays an important role in the safe and efficient operation of urban rail transit. How to ensure the high-reliability operation of the signal system has become an important issue for operation and maintenance personnel [5].

In previous studies, Yan and Tang [3] introduced the state-of-the-art development of the safety technologies for rail transit signal system. Wang [5] analysed the impact of signal system failures on operations, and discussed several solutions to improve the reliability of the signal system. Wang [6] et al. analysed and compared two methods for improving the reliability of the signal system, involving the combination of CBTC (communication-based train control) and BM (fixed block-based intermittent automatic train protection mode) and the combination of CBTC and TBTC (track circuit-based train control system) method. Yang [7] introduced two redundant switching methods for on-board ATC (automatic train control) systems. Wang [8] introduced two schemes on the selection and switching between main machine and standby machine that can be used in double 2-vote-2 redundancy and dual-system hot standby redundancy, and analysed and compared the advantages and disadvantages of the two schemes. Aiming at the influence of the failure of an axle counting host on the turn-back process, Lv [9] proposed a redundant control scheme for axle-counting systems. In this scheme, two axle counting hosts respectively collect pulse signals from the axle counting heads related to the turnout section, and after processing by the processor, the occupancy/idle and disturbed status of the turnout section are redundantly output to the computer interlocking system. Wu [10] analysed the switching process, implementation principle, implementation circuit, safety analysis and application cases of a primary and secondary redundancy scheme for VOBC (vehicle on board controller). Starting from market demand, the scheme realizes the complete redundancy of all VOBC equipment including external equipment, and solves technical problems such as undisturbed switching. Gan [11] introduced the principles of software redundancy and hardware redundancy in urban rail transit signal systems, discussed the redundant technical schemes in the modern urban rail transit signal system, and analysed the equipment redundancy and communication redundancy for the URBALISTM system as an example.

In addition, combined with the characteristics of the rail transit signal system after the transformation, in view of the reliability assessment requirements of the heterogeneous redundant architecture, Li et al. [12] suggested a Markov model of the heterogeneous redundant architecture, and derived a reliability evaluation model for the architecture. Zhang et al. [13] discussed a reliability evaluation method suitable for the double 2 redundant platform of the rail transit signal system.
3. Design

3.1. Main architecture
As shown in Figure 1, this system is composed of CBTC equipment and TBTC equipment (i.e., CBTC+TBTC), both of which share ATS (automatic train supervision) and interlocking equipment. CBTC wayside equipment and TBTC wayside equipment work independently, each providing movement authorization information and speed codes to control trains. The train-to-ground wireless network in the CBTC equipment uses two different wireless systems, including Wlan (wireless local area network) and LTE (long term evolution). The CBTC wayside subsystem interacts with the CBTC on-board subsystem via the wireless red and blue network for train control information. TBTC exchanges train control information with the TBTC on-board subsystem via the track circuit.

![Figure 1. Schematic diagram of system architecture](image)

3.2. Core scenarios
In order to minimize the impact of signal system failures on normal operations, this paper proposes a design of CBTC+TBTC system to ensure that when any system fails, it will not affect the normal operation of the train. Specifically, when the train-ground wireless communication equipment, antenna, wayside equipment, train location, or speed measurement equipment of CBTC fails, the train control will automatically switch to TBTC, and the emergency braking will not be triggered. Similarly, when the TBTC equipment fails, the train control will automatically switch to CBTC, and emergency braking will not be triggered. With this complete heterogeneity and hot standby redundancy, the availability of the system is greatly improved. The core scenarios of the system are as follows:

Scenario 1: Both the CBTC and the TBTC work normally. As shown in Figure 2, the contents involved in the scenario are:

- The CBTC is working based on the principle of mobile blocking. It is actively positioned by the train through the ground beacon (transponder). Wayside CBTC equipment provides movement authorization via train-ground wireless. The on-board CBTC equipment calculates the triggering speed of the emergency braking in real time according to the movement authorized destination.
- The TBTC is working based on the principle of fixed blocking. The track circuit detects the occupation of a train. The wayside TBTC equipment calculates the speed code and transmits it to the on-board TBTC equipment through the track circuit. The on-board TBTC equipment controls the train speed not to exceed the speed code, which is the trigger speed of FSB (full service brake). When the FSB is triggered, and the braking rate does not drop to the specified value, the emergency braking will be output.
The two sets of equipment monitor the speed of the train separately, calculate the emergency braking command independently, and the two are connected in parallel to the emergency braking loop of the train via an external circuit. Since each set of equipment can calculate the speed that the train need complied with, the train only apply emergency braking when both sets of equipment output emergency braking.

Scenario 2: The CBTC fails, but the TBTC works normally. As shown in Figure 3, in this scenario, the on-board CBTC system will output emergency braking, and the on-board TBTC system will not output emergency braking. Therefore, the train will not be subjected to emergency braking, which improves the availability of the system. If the train speed continues to exceed the TBTC speed code, the train will apply FSB to ensure the safety.

Scenario 3: The TBTC fails, but the CBTC works normally. As shown in Figure 4, in this scenario, the on-board TBTC system will output FSB and emergency braking, while the on-board CBTC system will not output emergency braking. Therefore, the train does not apply emergency braking, which improves the availability of the system. If the vehicle speed exceeds the CBTC speed profile, the train will apply emergency braking to ensure safety.
Scenario 4: Switching of train operation function. In normal operation, the actual train speed is below the CBTC speed profile and TBTC speed codes, and the traction and braking functions of the automatic train operation (ATO) subsystem are controlled by the CBTC system. When the CBTC fails, the traction and braking functions of the ATO are automatically switched to the TBTC system. When the CBTC failure is restored and its ATP (automatic train protection)/ATO mode is available, the traction and braking functions of the train is switched back to CBTC again.

3.3. Operation realization

The on-board equipment of CBTC and the on-board equipment of TBTC use a device for ATP protection. The on-board equipment of CBTC and TBTC provide EB (emergency braking) junction respectively, which are connected in parallel to the EB loop. The train only perform emergency braking when both systems output EB. The on-board equipment of TBTC provides an FSB junction, and the CBTC system provides another EB junction, which is connected in parallel to the FSB loop. When the CBTC system outputs EB, the FSB output by the TBTC system will be executed by the train.

The auxiliary operation part of the train uses a device to switch between the on-board ATO of the CBTC and the on-board ATO of the TBTC. During normal operation, the train operation is controlled by the on-board ATO of the CBTC. When the CBTC on-board equipment is completely faulty, the CBTC outputs emergency braking, or the CBTC-ATP/ATO mode is unavailable, the system will automatically switch to the on-board ATO of the TBTC to control the train operation.

The input and output interfaces of the train adopt automatic control mode. The inputs, such as operation mode, door status, and ATC cut-off status, are collected in parallel using the device shown in Figure 5. Signal commands, such as traction braking and door opening/closing, are output by the two systems at the same time, but they are switched by the switching unit. Wherein, the switching unit includes a relay, and the coil of the relay is connected in series in the CBTC loop. When the system is normal, the working junction of the on-board equipment of the CBTC is closed to drive the relay in the switching unit, and the function command received by the train comes from the on-board equipment of the CBTC. When the on-board equipment of the CBTC fails, the working junction is disconnected, the relay of the switching unit loses power, and the contact is switched to the TBTC system. The function commands received by the train are from the on-board equipment of the TBTC. The switching is performed automatically by the system.
The driver-machine unit switching control is shown in Figure 6. A CBTC/TBTC switch is set on the driver platform. The switch has two positions, i.e., "Automatic" and "TBTC". The working junction can be manually forcibly disconnected to switch the relay junction contact to the on-board equipment of the TBTC. Under normal condition, the switch is in the automatic position, and the on-board equipment of the CBTC controls the display of the DMI (driver-machine interface) and the mechanical speedometer. The DMI displays whether the current control system is the CBTC or the TBTC. When the on-board equipment of the CBTC fails, the system automatically switches to TBTC via the switching unit, and the on-board equipment of the TBTC controls the mechanical speedometer.

At the same time, the TBTC and CBTC are independently set up for wayside equipment other than ATS and interlock. Therefore, neither a single TBTC failure nor a CBTC failure will affect the operation of the train. Among them, the on-board equipment of the CBTC can implement a head and tail redundancy strategy, the external equipment of each end includes speed measurement device, beacon antenna, and wireless communication antenna (a set of LTE and a set of Wlan). The on-board equipment of the TBTC can implement a single-ended redundancy strategy, the external equipment includes speed sensor, track circuit receiving antenna, TWC (train-wayside communication) antenna, parking coil antenna, and sign coil antenna.
3.4. Effect analysis
First of all, taking the train-ground communication failure as a trigger condition, the state transition process of the train control system is discussed via Markov process [6]. The RAM (reliability, availability, and maintainability) indicators referenced in the analysis are mean time between failures (MTBF), failure rate and reliability. The results based on a simulated train running with 1000 hours showed that the mean time between failures is 100004 h, the failure rate is 10.0, and the reliability is 0.999995. The results suggest that the system has high availability.

In addition, in view of the improvement of train delays caused by the discussed signal system, a timed Petri net was used to establish the process of switching the control system from CBTC to TBTC [6]. Among them, we suppose that when the DCS (data communication subsystem) of the CBTC fails, the train is immediately connected to the TWC (train-wayside communication) equipment of the TBTC to realize continuous communication. Considering that train delays are mainly caused by the increase of train running intervals and the decrease of train speed, the train delay time caused by the degraded train control system is calculated according to the constructed timed Petri net model. Based on the Petri net model, when the operation design interval is set to 100 s, 120 s, and 180 s, a series of train delay times are obtained. Specifically, when the operation design interval is 100 s, the train delay time does not exceed 2 min. When the operation design interval is 120 s and 180 s, the train delay time does not exceed 5 min.

Since the system is a blocking system with continuous communication, and has a complete redundant structure, the signal switching time when it is degraded is only caused by its own driving interval and speed degradation. Therefore, the above results are expected, and the proposed design is effective and feasible, which helps to improve the availability of the system.

4. Conclusion
This paper discussed a system-level heterogeneous hot standby redundant signal system, involving a CBTC system, a TBTC system, and a switching unit. The CBTC and TBTC can respectively communicate with the train through the switching unit. The design has the following advantages: 1) Not only does redundancy design at the device level, but also realizes heterogeneous hot standby redundancy at the system level. 2) The switching is performed automatically, without manual intervention. 3) The availability of the system is improved, the impact of failures on operations is reduced, and the quality of service is guaranteed. 4) For retrofit projects, existing track circuit-based systems can be reused, and existing investments can be effectively utilized.

Acknowledgments
This work was jointly supported by the Science Research Project of Shanghai Science and Technology Committee (Grant no. 18DZ1205803), the National Key R&D Program of China (Grant no. 2016YFB1200602-02), the Foundation of Shanghai Maglev and Rail Transit Cooperative Innovation Center (Grant no. 20132223), and the R&D Project of Shanghai Shentong Metro Group Co., Ltd. (JS-KY19R012-WT-20018).

References
[1] Sun, L., Hong, H., Shi, C., et al. (2019) Contradiction and unity between railway operation safety, service safety and information safety. Urban Mass Transit, 22(6): 15-19.
[2] Farooq, J., Soler, J. (2017) Radio communication for Communications-Based Train Control (CBTC): A tutorial and survey. IEEE Communications Surveys & Tutorials, 19(3): 1377-1402.
[3] Yan, F., Tang, T. (2005) Research and development of safety technology in signalling system of rail transit. China Safety Science Journal, 15(6): 94-99.
[4] Pan, L. (2019) Analysis of reliability model of CBTC signal system in rail transit. Electronics World, 20(17): 5-8.
[5] Wang, X. (2016) Reliability analysis for signal system of urban rail transit. Railway Signalling
& Communication, 52(11): 68-71.
[6] Wang, X., Ou, D., Liu, Y., et al. (2021) Reliability and operation availability analysis of heterogeneous redundancy train control system. Urban Mass Transit, 24(4): 1-5.
[7] Wang, Z. (2018) On the redundant switchover scheme of on-board controller in urban rail transit signal system. Urban Mass Transit, 21(z1): 17-19.
[8] Yang, L. (2019) Comparative analysis of on-board ATC control system redundancy modes in urban transit. Modern Urban Transit, 16(11): 28-32.
[9] Lv, H. (2018) Redundancy control scheme of urban rail transit axle counting system in turn-back area. Urban Mass Transit, 21(z1): 79-82.
[10] Wu, L. (2017) Research on main use and reserve VOBC head to tail redundancy switching scheme. Urban Mass Transit, 20(z1): 66-67.
[11] Gan, Y. (2012) Analysis of redundancy technology in urban rail transit signal system. Urban Mass Transit, 15(5):110-113.
[12] Li, M., Zhang, H., Liu, X., et al. (2021) Research on heterogeneous redundancy reliability evaluation model of rail transit signal system. Railway Signalling & Communication, 57(3): 80-83.
[13] Zhang, H., Li, M., Qin, J., et al. (2019) Research on static and dynamic reliability evaluation of double 2 platform of rail transit signal system. Electronics World, 21(19), 9-12.
[14] Wang, X., Xu, Y. (2019) A system-level heterogeneous hot standby redundant signal system. CN106564517B.