Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/87/20241523

Communication security analysis of fully electronic interlocking systems

Xiyan Hou

Key Laboratory of Photoelectric Technology and Intelligent Control of the Ministry of Education, Lanzhou Jiaotong University, Lanzhou, China

2073787258@qq.com

Abstract. Communication security in fully electronic interlocking systems is one of the key factors ensuring the safe and reliable operation of the entire system. EN50159 is an important standard in the European railway communication sector, aimed at ensuring the safety, reliability, and efficiency of railway transportation. According to the communication security standards of EN50159, there are six types of security risks in closed communication: data duplication, deletion, insertion, misordering, delay, and corruption. This paper analyzes and explains the aspects of communication security that need to be considered based on the safety communication standards of China's railway signaling system and the signal safety standards in EN50159, focusing primarily on communication security and reliability.

Keywords: Fully electronic interlocking system, EN50159, closed communication, communication security

1. Introduction

With the rapid development of computer networks and communication technology, railway signaling systems have greatly improved, making train operations faster, safer, and more efficient. The advent of new technologies in modern communications and microelectronics has accelerated the development of computer networks and communication technology, driving continuous upgrades in railway signaling technology. Communication-based train control systems have seen broader application, though the relationships between railway signaling systems have become more complex [1]. The adoption of advanced fully electronic computer interlocking systems, which no longer rely on traditional gravity-based safety relays but use electronic execution units for ultimate control, offers significant advantages in terms of maintainability, reduction of control room area, and construction workload. These systems have become the mainstream direction for railway signal control systems in China [2]. Given their high safety and real-time requirements, the operating cycle of fully electronic computer interlocking systems must be less than 250ms, and the safety performance must meet the SIL4 standard [3].

2. Safety Communication Standards

Railway communication systems are primarily used for train control, signal transmission, personnel communication, and emergency rescue. These systems must be highly reliable, stable, and resistant to interference to ensure the safety and smooth operation of railway transport. With the establishment of safety standards, international organizations have developed various versions of safety communication protocols tailored to different train control systems, transmission networks, and defense against attacks, ensuring communication safety in railways. EN50159 is a crucial standard in the European railway communication field, aimed at ensuring the safety, reliability, and efficiency of railway transportation. It provides a comprehensive safety assurance system for railway information transmission systems with its strict functional requirements and technical specifications [4]. The EN50159 standard includes requirements for the design, installation, operation, and maintenance of communication systems, providing a unified reference framework to ensure compatibility and interoperability among different systems within the railway industry. This standard covers various communication technologies, including wired and wireless communication systems, and equipment related to train control, signal transmission, and personnel communication. To ensure secure communication transmission, we must strictly adhere to security communication protocols and ensure the stability of the characteristics of the closed transmission system, so that the number of connected devices and the maximum data capacity are not affected [5], thereby reducing the risk of illegal interference.

To ensure the safety of closed transmission systems, we must detect and prevent risks such as data frame overlap, omission, insertion, confusion, error, and timeout as early as possible. These risks include, but are not limited to, transmission system failures and external influences. Therefore, before designing communication protocols, it is essential to carefully review the characteristics of data frames for accuracy, reliability, orderliness, and timeliness to ensure the entire communication system meets safety communication requirements [6].

3. Fully Electronic Computer Interlocking System

3.1. Fully Electronic Computer Interlocking System Architecture

In traditional railway signaling systems, train operations are manually controlled by signal operators. In contrast, fully electronic computer interlocking systems achieve signal control and train dispatch through electronic devices and computer software. These systems have significant advantages in improving operational efficiency, reducing human error, and enhancing safety [7]. The fully electronic computer interlocking system typically consists of the following main components [8]:

1. **Computer System:** Responsible for controlling and managing the entire interlocking system, including functions such as processing train location information and signal control commands.
2. **Interface Equipment:** Communicates with track equipment, signal devices, and train location detection devices to obtain real-time train location and status information.
3. **Interlocking Logic Control Unit:** Formulates signal control logic based on train location, dispatch plans, and other information to ensure safe and smooth train operations.
4. **Communication Equipment:** Facilitates communication among various parts of the system, including data transmission and command delivery.
5. **Human-Machine Interface:** Provides an interface for operators to monitor and manage the system. Typically, it displays train locations, signal status, and other information on a computer screen, allowing operators to take appropriate actions based on system prompts.

In summary, the structure of the fully electronic computer interlocking system is shown in Figure 1. The fully electronic communication layer communicates with the electronic control module layer via a bus, and both the interlocking logic layer and the fully electronic communication layer adopt a 2x2 redundancy structure. The electronic control module layer uses a dual-machine hot standby structure, with both the interlocking machine and the communication machine employing safety computers [9].

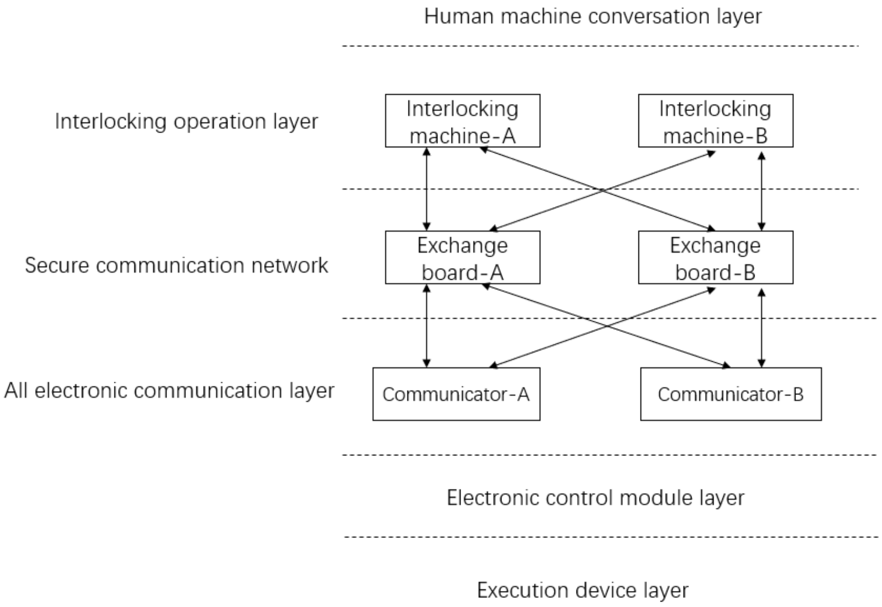
Human machine conversation layer
Interlocking operation layer
Interlocking machine-A
Interlocking machine-B
Secure communication network
Exchange board-A
Exchange board-B
All electronic communication layer
Communicator-A
Communicator-B
Electronic control module layer
Execution device layer

Figure 1. Structure of the Fully Electronic Computer Interlocking System

3.2. Safety Communication Requirements of the Fully Electronic Computer Interlocking System

The safety communication network of the fully electronic interlocking system is designed for communication between the interlocking machine and the communication machine, forming a closed transmission network [10]. It follows the EN50159 technical standard set by the European Committee for Electrotechnical Standardization (CENELEC) to ensure safety at railway crossings. EN50159 is an important standard in the European railway communication signaling field, outlining the basic requirements for safe communication protocols to ensure system safety and reliability. Currently, some European equipment or system solutions used in China's train control systems involve the safety communication system and interface protocol established by the EN50159 standard. This standard not only clearly identifies the potential dangers of closed transmission systems but also determines the best protective measures based on this technical standard to ensure railway operational safety [10].

According to the EN50159 standard, in a closed communication environment, to reduce threat risks, safety function modules are generally embedded in the application layer and the communication protocol data layer to implement safety protocols. The safety function modules can provide four types of verifications: authenticity, integrity, timeliness, and orderliness of messages. That is, received data is handed over to the application layer only after passing the safety function module verification; data to be sent by the application layer is packaged by the safety communication module before being transmitted externally [11-12]. Therefore, we must ensure that every part adheres to strict safety regulations and take appropriate measures to protect them. This ensures a secure and reliable communication service environment. The position of the safety communication protocol in the safety communication model is shown in Figure 2.

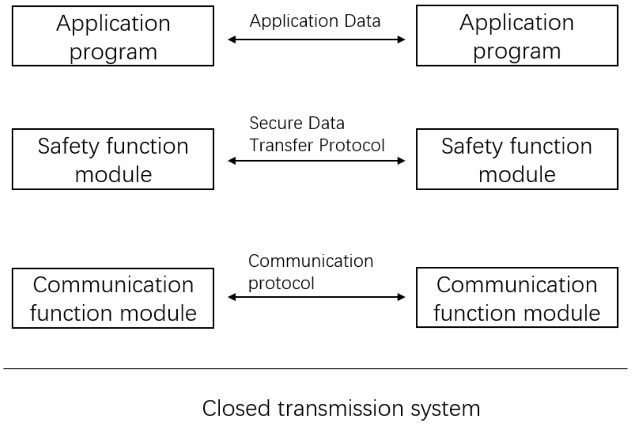

Figure 2. Safety Communication Model

To ensure the safety and reliability of the internal communication system, we divide it into three layers: the application layer, the safety protocol layer, and the communication base layer. Each layer defines the respective data formats. The application layer is responsible for processing the actual data required for interactions. The safety protocol layer ensures communication reliability and is designed according to the EN50159 standard. Finally, the communication base layer stores data in the inherent format specified by the device bus [13].

4. Communication Security Analysis of the Fully Electronic Computer Interlocking System

4.1. Analysis of Communication Security in the Fully Electronic Computer Interlocking System

Communication security in the fully electronic computer interlocking system ensures the safety of communication between different parts of the system to prevent unauthorized access, data leaks, or tampering [14]. To analyze the communication security of the fully electronic computer interlocking system, the following aspects are typically considered:

1. Encrypted Communication: Ensuring that data transmitted between different parts of the system is encrypted to prevent data theft or tampering. Common encryption algorithms include AES and RSA, which ensure data confidentiality during transmission.

2. Identity Authentication: Verifying the identities of users and devices within the system to ensure that the communicating parties are legitimate and trustworthy. Identity authentication mechanisms can prevent unauthorized access.

3. Access Control: Restricting user or device access to system data and functions to ensure that only authorized users can perform specific operations. Detailed access control effectively reduces potential security risks.

4. Firewalls and Intrusion Detection Systems: Setting up firewalls and intrusion detection systems within the system to monitor network traffic and behavior, quickly identifying potential attacks and preventing or alerting them in time.

5. Security Vulnerability Management: Regularly scanning and assessing the system for security vulnerabilities and promptly patching known vulnerabilities to maintain system security continuously.

6. Logging and Auditing: Recording operation logs within the system, including user logins, data access, and other behaviors, to trace and investigate security incidents when they occur.

7. Physical Security: Ensuring the physical security of the system's servers and network equipment to prevent unauthorized personnel from accessing and operating system hardware.

By comprehensively considering these factors, the communication security of the fully electronic computer interlocking system can be effectively guaranteed [15]. Additionally, continuously monitoring the latest developments and technologies in the security field and promptly adjusting and updating security strategies are crucial for maintaining system security.

4.2. Reliability Analysis of Communication in the Fully Electronic Computer Interlocking System

Reliability analysis of communication in the fully electronic computer interlocking system is crucial to ensure that data and commands are transmitted stably and efficiently during the communication process [16]. The following are common methods and strategies for evaluating and enhancing the reliability of communication in the fully electronic computer interlocking system:

1. Fault Analysis and Fault Tolerance Design: Analyzing and predicting potential communication failures in the system, designing fault tolerance mechanisms to handle communication failures, ensuring that the system can automatically switch to backup channels or recover to normal operation in case of issues.

2. Communication Link Quality Monitoring: Monitoring the quality and stability of each communication link in the system, including metrics such as delay, packet loss rate, and bandwidth utilization, to identify and adjust for communication problems promptly.

3. Data Integrity Check: Introducing verification mechanisms, such as CRC checks, during data transmission to ensure data integrity and prevent data corruption or tampering.

4. Redundant Communication Design: Implementing redundant communication paths or devices to achieve backup and redundancy in communication, enhancing system reliability and stability. If the primary communication path encounters problems, it can quickly switch to the backup path.

5. Network Topology Design: Designing a reasonable network topology to avoid single points of failure affecting the entire system's communication. Adopting distributed architectures and multi-path communication to improve the system's resistance to interference.

6. Communication Security Strategies: Implementing security measures such as encrypted communication, identity authentication, and access control to protect communication data security and prevent information leaks and attacks.

7. Regular Maintenance and Monitoring: Performing regular maintenance and monitoring of the system's communication equipment and network to detect and address potential issues promptly, ensuring the system's stability and reliability.

By comprehensively applying these measures and strategies, the communication reliability of the fully electronic computer interlocking system can be effectively enhanced, ensuring stable and efficient data transmission and command control during system operation [17-18].

5. Conclusion

In railway transportation, the train interlocking system ensures the safe and smooth passage of trains through intersections, shunting lines, and other sections to avoid accidents and collisions. The fully electronic computer interlocking system introduces modern electronic and computer technologies, improving the intelligence and safety of the railway transportation system while enhancing the efficiency and accuracy of train operations. Therefore, ensuring stable communication in the fully electronic computer interlocking system and providing a secure communication environment has become paramount in ensuring the normal operation of the railway control system.

References

[1] Ma Jun. Analysis and Research on Modern Railway Signal System [J]. SME Management and Technology (Late Issue), 2016, (02): 276.

[2] Duan Wu. Overview of the Development of Railway Station Interlocking in China [J]. Railway Communication Signal, 2019, 55(S1): 86-97.

[3] Fu Limin. Research on the Development and Application of Fully Electronic Interlocking [J]. Railway Communication Signal Engineering Technology, 2020, 17(03): 32-38.

[4] A. Nouri and J. Warmuth, "IEC 61508 and ISO 26262 - A Comparison Study," 2021 5th International Conference on System Reliability and Safety (ICSRS), Palermo, Italy, 2021: 138-142.

[5] DIN EN 50159-2011, Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems; German version EN 50159:2010[s].

[6] Hassan Md Kamrul, Subramanian Kannan Bala, Saha Swapan, Sheikh M. Neaz. Behaviour of prefabricated steel-concrete composite slabs with a novel interlocking system – Numerical analysis [J]. Engineering Structures, 2021, 245.

[7] W. Fu, K. Wang, H. Feng and X. Ma, "Research on Computer Interlocking System with Interoperability Function," 2019 IEEE 2nd International Conference on Electronics and Communication Engineering (ICECE), Xi'an, China, 2019, 230-234.

[8] Lee J, Jung J. Verification and Conformance Test Generation of Communication Protocol for Railway Signaling Systems [J]. Computer Standards & Interfaces, 2007, 29(2): 143-151.

[9] Han Bingqian, Su Xiuyuan. Research on the Development and Application of Fully Electronic Interlocking System [J]. Railway Communication Signal Engineering Technology, 2022, 19(08): 92-96.

[10] Wang Yuetai, Wu Wen'ai. Analysis of Reliability and Safety of Computer Interlocking System [J]. Inner Mongolia Coal Economy, 2020, (05): 159.

[11] Zhang Hanbai. Communication Protocol Scheme and Security Impact in Fully Electronic Computer Interlocking System [J]. Digital World, 2019, (02): 26.

[12] H. Feng, J. Yu, X. Mo, M. Song and Y. Guan, "Research on All Electric Computer Interlocking System," 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 2021, 406-410.

[13] Xu Li, Su Siqi, Kuang Wenzhen. Design and Security Analysis of Communication Protocol for Fully Electronic Computer Interlocking System [J]. China Railway Science, 2012, 33(06): 83-87.

[14] Pinedo C, Aguado M, Lopez I. Modelling and Simulation of ERTMS for Current and Future Mobile Technologies [J]. International Journal of Vehicular Technology, 2015, 2015: 1-11.

[15] Franco D, Aguado M, Pinedo C. A Contribution to Safe Railway Operation: Evaluating the Effect of Electromagnetic Disturbances on Balise-to-BTM Communication in Railway Control Signaling Systems [J]. IEEE Vehicular Technology Magazine, 2021, 16(2): 104-112.

[16] Yin Qin, Zhang Liwei. Implementation Method of Secure Communication Protocol Based on Open Network [J]. Railway Communication Signal Engineering Technology, 2023, 20(01): 24-27+45.

[17] Feng Haonan. Design and Research of Fully Electronic Computer Interlocking System for Urban Rail Transit [J]. Journal of Railway Science and Engineering, 2021, 18(08): 2145-2155.

[18] Gao Yang, Luo Yangfan. Discussion on Security Requirements of Wireless Communication Protocol for High-speed Railway [J]. China Railway, 2022, (11): 123-128+134.