Research on Synchronous Network Platform of Rail Transit Signal System Based on Beidou Satellite Navigation

Xiping Yu
Wuhan Railway Vocational College of Technology, China
603718609@qq.com

Abstract. The signal system is an important part of the modern high-volume, high-density rail transit automatic control system, ensuring the safety of trains and passengers, and plays an important role in the high-speed and orderly operation of trains. The paper introduces the latest development and latest requirements of the synchronous network technology of the rail transit communication system; proposes the construction strategy of the urban rail transit network level synchronization network based on the Beidou satellite navigation system; improves the localization rate of the system and realizes the line network level.

1. Introduction
The signal system is one of the most basic control systems for urban rail transit. It is the key system to ensure the safe operation of trains, realize the automation of train operation and modernization of driving command, and improve operational efficiency. The signal system is an important part of the modern high-volume, high-density rail transit automatic control system, ensuring the safety of trains and passengers, and plays an important role in the high-speed and orderly operation of trains. Blocking technology is a core technology in signal systems. Occlusion means that in order to ensure the safety of train operation and prevent train collision and rear-end collision, only one train is allowed to be occupied within the same time zone (i.e., the train has entered the section or the train has not entered the section, but the occupation of the occupied section has been obtained) The method taken to meet this technical requirement. In recent years, with the increasing application and deepening of computer systems in signal systems, signal systems are developing in the direction of network and intelligence [1].

However, at present, the domestic rail transit clock synchronization system generally adopts a GPS satellite navigation system, and the localization rate is low. In order to meet the development needs of the rail transit network, it is urgent to establish a unified line-level clock synchronization network platform with high localization rate to realize the time and clock synchronization of the weak current systems of each line. With the construction and improvement of China Beidou satellite navigation system, its comprehensive service capabilities, such as service area, positioning accuracy and anti-interference ability, have been significantly improved. Fully meet the functional requirements of the rail transit synchronization network. However, considering that the Beidou navigation system is not fully mature, the rail transit synchronization network of a city can be temporarily considered as the main scheme of GPS+ Beidou navigation.
2. Safety analysis of the synchronization platform of rail transit signal system

For the urban rail transit signal system, the goal of information security is to provide a "sexual good" environment for the life cycle of information storage, transmission and processing in the signal system, and the signal system itself must be from the concept of "sexual evil" Design to improve the robustness of the system. Signal systems differ from the principles of information security objectives of traditional general information technology systems [2]. As shown in Table 1, traditional general information technology systems follow CIA principles, while signal systems follow AIC principles.

Table 1. Signal System and General Information Technology System Information Security Objectives Follow Principles Table

| operating system                                      | Information security objective principle          | Principle name |
|--------------------------------------------------------|--------------------------------------------------|----------------|
| Industrial control system (signal system)              | Availability > Integrity > Confidentiality       | AIC            |
| General information technology system                  | Confidentiality > Integrity > Availability       | CIA            |

The information security threats faced by industrial control systems fall into five categories: 1 environmental and natural threats; 2 internal unintentional threats; 3 internal intentional threats; 4 external attacks; 5 third-party personnel, with backdoors, and third-party personnel in the system During maintenance, changes to the system or installation of illegal software may not be authorized [3].

1) System Vulnerabilities: After extensive use of general-purpose protocols and general software and hardware, industrial control systems are still designed, developed, configured and managed based on dedicated, closed operating environments, without system protection, access control, and system integrity. Safety indicators such as data confidentiality were included, resulting in a large number of loopholes introduced in the industrial control system.

2) Intrusion and attack: The invasion and attack methods of the industrial control system are extremely concealed, complicated, and have a long latency period. They are highly targeted and severely destructive, such as the Stuxnet, the Duqu, the Flame, etc. virus.

3) The protective measures are weak and the security awareness is not strong: because the industrial control system pays more attention to the usability and the convenience of operation, the passwords of the devices (especially network devices) in the system are generally weak and lack of updates, and the management system of the mobile media is difficult. Long-term implementation; lack of strict security measures, may lead to unauthorized access, the system is infected with worms, Trojans and other malicious programs, bringing risks to the safe operation of the system.

3. Line network level synchronization network platform construction plan

The urban rail transit network level synchronization network can be constructed in a five-layer architecture, as shown in Figure 1. The first layer includes GPS receiving equipment, Beidou satellite receiving equipment, first-class time server and first-level network management equipment. The main and standby systems should be set in the rail transit network command center and the alternate line network command center. The second layer is the weak current system host located in each line control center, and the NTP protocol is used in the time synchronization network; the third layer is the slaves connected to the station host at each station of the weak current system, and also in the time synchronization network. Use the NTP protocol [4].

The system adopts the above layered architecture, which has the following advantages: 1 Each subway line complies with the same synchronization source (i.e., layer 1 time server equipment), ensuring uniform time of the entire network; 2 avoiding the construction of various subway lines At the same time, satellite navigation system equipment is set up, the investment of construction is reduced, and the resource sharing of satellite navigation system equipment is realized; 3 system layered architecture, level-by-level protection, superior system equipment failure, the next level system can still use this level The punctuality equipment works to improve the reliability of the system; 4 The GPS + Beidou interactive satellite navigation system is used to improve the localization rate of the system.
3.1. Network synchronization

The main working principle of the time synchronization system of this solution is to adopt a layered architecture and multi-level protection. That is: when the system's Layer 1 equipment, satellite navigation system failure, BITS failure, the first-level server can still work with its own crystal oscillator. The two primary time servers are mutually active standby. When two primary time servers fail, the system synchronizes the time based on the Layer 2-time device. By analogy, when the first, second, third, and fourth layer time system devices are faulty, or communication with the upper layer device is interrupted, each subsystem in the line network that needs clock synchronization needs to be used by the system host's own crystal oscillator. Synchronize.

3.2. Time precision synchronization

The synchronous clock source of the switching, transmission and other devices at the core node of the transmission system core layer is taken from the clock output module of the BITS system of the core node. The clock synchronization signal of the core layer transmission node uses the clockwise line clock signal sent from the GPS set point BITS as the master clock to take the counterclockwise line clock signal from the BITS of the clock source as the standby clock. The clock synchronization signal of the transmission node in the convergence layer line transmission system is extracted from the line code stream in the ring, and the main clock signal is extracted from the interconnection line code stream between the core transmission equipment and the line transmission equipment of the line control center. The hour hand line clock signal; the standby clock signal is a counterclockwise line clock signal extracted from the interconnect line code stream between the control device and the line transmission device of the line control center.
4. Design of information security in signal system

Signal system security is a complex system engineering, including functional safety, information security, and physical security. The signal system itself pays more attention to functional safety; while information security and physical security protect the signal system and provide a "good" environment. The relationship is shown in Figure 1. Information security management systems, management systems, physical security, secure network architecture, detection and detection, and data security are all areas of information security; application security is functional security under information security.

As shown in Figure 2, the security of the management category has clear specifications and control points in the security and industrial control system information security IEC62443 standard; the physical security in the rail transit system can generally be met; network architecture security, monitoring, detection It is generally implemented by public information products provided by professional information security vendors. The article mainly designs information security from the aspects of data security and application security that are strongly correlated with signal systems and strongly coupled.

4.1. Rail transit signal system Improvement of RSSP-II protocol

The RSSP protocol is a secure communication protocol for railway signal security device interfaces. The RSSP-I protocol is for closed networks and the RSSP-II protocol is for open networks. The domestic autonomous urban rail transit signal system generally adopts the RSSP-II secure communication protocol, which adopts threat prevention measures such as serial number, time stamp, source and destination identifier, message authentication security code, etc., and can defend against the description in EN50159-2. The seven threats introduced by the open communication network [5].

The RSSP-II protocol uses a 3-fold DES encryption algorithm to implement identity authentication between communicating entities and message source verification/message integrity verification of service data, protecting against the risks of "damage" and "disguise". However, the plaintext + security code communication method used in the protocol does not provide any confidentiality protection for the signal system business data. When using the 3-fold DES encryption algorithm, a shorter key life cycle is required, and it is recommended to provide at most 30 minutes to provide sufficient security code.
protection for security-type business data. Because the 3 DES encryption algorithm itself is facing the risk of being cracked, it can be compensated by shortening the key life cycle at this stage. To completely eliminate the security risk of cracking, an encryption algorithm such as AES-256 anti-quantum computing attack is needed.

4.2. Data security design
The key data of the signal system mainly includes: 1 access authentication/identification data, such as username/password, private key, key, biometric data, etc.; 2 configuration data of key applications, such as line database, application configuration file, etc.; 3 system management data, such as user name, operation authority, etc.; 4 key business data, such as operation schedules, operational operation logs, etc. Signal system software uses both secure storage and integrity verification techniques to secure critical data. First, the system encrypts and stores critical data. Even if the host is illegally accessed or the storage medium is illegally acquired, the intruder cannot obtain the key data or obtain the available information of the further attack signal system from the key data. Secondly, these key data stores carry the MAC code [6]. When the software reads these key data, only the universal MAC authentication can be used. Therefore, any tampering and damage to the key data will be detected and alarmed. The disaster recovery of key data uses the medium periodic backup mode or the synchronous transmission off-site storage mechanism, and can be restored immediately after the data is tampered with and damaged.

4.3. Encrypted transmission of information
Trusted networks are mainly independent closed networks dedicated to signal systems; non-trusted networks include open standard vehicle-to-ground wireless transmission systems, integrated bearer networks, public wireless networks/Internet (for portable mobile maintenance terminals, remote Web workstations, etc.). When the signal system security related data is transmitted in the untrusted network, the data encryption technology and the dynamic access authentication technology against the quantum computing attack are adopted to ensure the confidentiality of the data transmission and the legitimacy of the session. The encryption algorithms that can be used include the domestic ancestral encryption algorithm and AES-CBC, AES-GCM, and the key length can be 256 bits at this stage. The security of encryption depends not only on the encryption algorithm itself, but also on the security of key management. Reduce the involvement of people in the key management process through technical means. Key generation protocols such as IKEv2 or SRP6 are used to manage the generation, distribution, update, and destruction of keys.

![Figure 3. Data encryption transmission](image)

4.4. Application Access Control and Access Authentication Security Design
For the security protection of hosts and applications, the current user name/password access control policy is upgraded to two-factor authentication to provide access protection and usage control security. Biometrics technology is very mature and widely used in finance, security and other fields. Applying biometrics to the operation and management of rail transit signal systems requires a combination of operational procedures and operational habits. At the same time, it is necessary to optimally design an access/access control strategy. In an emergency, the dispatcher can temporarily modify the access. /
Access control strategy. Biometric technologies currently available include face recognition, iris recognition, fingerprint recognition, and the like. Especially for remote terminal equipment, it must pass two-factor/multi-factor authentication.

5. Conclusion
The scheme adopts a three-layer architecture to build a synchronous network system, which solves the problem of time synchronization of the whole network, saves construction investment, and realizes resource sharing at the line network level. The first-level time server adopts the GPS+Beidou double-star main standby mode, which improves the reliability and localization rate of the system. With the improvement of China's Beidou satellite navigation system, its timing, positioning and other technologies will also be widely used and developed in the rail transit industry, which is of great significance in localization, security and confidentiality.

References
[1] Duan Longfei, Jiao Aiping, Jiao Aijun, et al. Safety and Construction Joint Control of Green Rail Transit System under Beidou Time Series. Academic Salon of Integrated Rail Transit System. Vol. 4 (2015) No.28, p. 103 - 105.
[2] Shi Jun. Discussion on the Security Encryption Mechanism of Urban Rail Transit Signal System Network Transmission. Science and Technology Information, Vol. 6 (2013) No.15, p. 296 - 299.
[3] Jing Jingli. Research on Clock Synchronization of Urban Rail Transit Signal System. Information Research, Vol. 5 (2017) No.4, p. 41 - 45.
[4] Niu Jingyi; Lu Manhong; Shao Shihai; Xu Qiang. Research on remote transmission technology of Beidou satellite RF signal based on commercial optical fiber line. The 9th China Satellite Navigation Academic Annual Conference. Vol. 7 (2018) No.45, p. 15 - 19.
[5] Cai Bogen, Fan Yuming, Wang Jian, et al. Research on Key Technologies of Rail Traffic Application Based on Beidou Navigation Satellite System. Excellent Papers of the 8th China Intelligent Transportation Annual Conference - Rail Transit. Vol. 12 (2013) No.21, p. 11 - 17.
[6] Zhao Hui. Discussion on the Application of Beidou Satellite Navigation System in Subway. Railway Technology Innovation, Vol. 2 (2018) No.14, p. 19 - 21.
[7] Cai Bogen, Shang Guanwei, Wang Jian, et al. Train Safety Location Support Method Based on Beidou Satellite Navigation System. China Railways, Vol. 5 (2013) No.12, p. 18 - 27.