Railway Cybersecurity in China

National Railway Administration of P. R. China
1. Overview

1.1 General information

- As of 2023,
  - China's railway operating mileage reached **159,000** km, including **45,000** km of high-speed rail, with passengers of about **3.68** billion
  - China's city railway transit mileage was **over 10,000** km, reached to **306** lines, covering **55** cities, **3.33** million trains, with passengers of about **2.67** billion
1. Overview

1.2 Trend

Goal: high efficiency and energy saving, environmental protecting, safe and reliable

The use of new technologies and applications, such as the IoT, cloud computing, and AI

Self-contained and closed, self-contained system

Open

Data sharing, data circulation

The cybersecurity situation is even more severe

Essential characteristics of IT network security

Confidentiality - Integrity - Availability

Essential characteristics of OT network security

Availability - Integrity - Confidentiality

Cybersecurity became an important topic
1. Overview

1.3 Challenges

- **Complex composition** of the system, large amounts of data interaction
- Cybersecurity includes including **physical** security, **network** security, **data** security and **personnel** security
- Traditional railway network architecture, the geographical distribution of railway transit infrastructure, and the **influence of old systems**, all these will lead to being difficult to improve cybersecurity
PART 02
Cybersecurity Practices
2. Cybersecurity Practices

2.1 Policies and regulations

At the national level, clear positioning and overall requirements are given.

- Network security and informatization are the wings of a bird, the wheels of a car, it must be uniformly planned, deployed, promoted and implemented.

- It is necessary to implement the responsibility for the protection of critical information infrastructure, with industries and enterprises assuming responsibility for the protection of the main body as operators of critical information infrastructure, and the competent departments performing their regulatory responsibilities.

Cybersecurity Law

Cryptography Law

Regulations on Classified Protection of Cybersecurity

The security implications are wider

Security construction penetrates all walks of life and various scenarios.

Key protection of critical infrastructure

As a key infrastructure that may affect the national economy, people's livelihood and public interests, rail transit implements key protection on the basis of the classified network security protection system.
2. Cybersecurity Practices

2.2 Network security protection

- It consists of two parts
  - Technical part mainly includes "one center, three protections"
  - Management part consists of five parts including safety management system etc.
### 2. Cybersecurity Practices

#### 2.3 Specific security measures

<table>
<thead>
<tr>
<th>Technical measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physical and environmental security</strong></td>
</tr>
<tr>
<td>✓ Physical isolation, physical disaster prevention, emergency power supply</td>
</tr>
<tr>
<td><strong>Communications network security</strong></td>
</tr>
<tr>
<td>✓ Network isolation, zone division, and border protection</td>
</tr>
<tr>
<td><strong>Industrial host security</strong></td>
</tr>
<tr>
<td>✓ Security software, patch upgrades, identity authentication, peripheral management</td>
</tr>
<tr>
<td><strong>Application security</strong></td>
</tr>
<tr>
<td>✓ Source code audit and security upgrade</td>
</tr>
<tr>
<td><strong>Data security</strong></td>
</tr>
<tr>
<td>✓ Classified and hierarchical management of data, differentiated protection, data backup, and test data protection</td>
</tr>
<tr>
<td><strong>Monitoring, early warning and situational awareness</strong></td>
</tr>
<tr>
<td>✓ Asset perception, risk monitoring, threat warning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management measures</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security planning and institution-building</strong></td>
</tr>
<tr>
<td>✓ Institutions and Construction, Strategies and Procedures, and Division of Responsibilities</td>
</tr>
<tr>
<td><strong>Personnel management and training</strong></td>
</tr>
<tr>
<td>✓ Personnel safety management, education and training</td>
</tr>
<tr>
<td><strong>Asset security management</strong></td>
</tr>
<tr>
<td>✓ Equipment asset management, media protection</td>
</tr>
<tr>
<td><strong>Supply chain security</strong></td>
</tr>
<tr>
<td>✓ Product selection, supplier selection, procurement delivery, contract agreement control</td>
</tr>
<tr>
<td><strong>Emergency response</strong></td>
</tr>
<tr>
<td>✓ Emergency plans, emergency drills</td>
</tr>
<tr>
<td><strong>Configuration management</strong></td>
</tr>
<tr>
<td>✓ Security configurations, configuration changes</td>
</tr>
</tbody>
</table>
2. Cybersecurity Practices

2.4 Use Case for Train

- **Firewalls at train network boundaries** for isolation protection, access control, and intrusion detection
- **Comprehensive audits of key nodes** within the train network
- **Security reinforcement measures** such as access control and log audit are adopted for on-board equipment
- **Analysis of historical data**, to achieve the real-time monitoring and visual display of train safety status
2. Cybersecurity Practices

2.5 Use Case for Train Control System

- Implement division of security zones, adding isolation protection and intrusion detection measures at the boundaries.
- Monitor and audit security within the internal subdomains of the business system.
- Implement antivirus, malware prevention, and log auditing on hosts and servers.
- Centralized control of security devices, system security policies, logs, and operations.

[Diagram of cybersecurity practices for a train control system]
2. Cybersecurity Practices

2.6 Use Case for Ground Information System

- Build security domains based on external service networks, internal service networks, and secure production networks, forming vertical protection mechanisms.
- Customize application security zones within the domain based on application system security needs.
- Implement bottom-up protection strategies from the physical link layer, network layer, to application layer at domain boundaries.

![Diagram showing security domains and boundaries]

- Internet/External Cloud Boundary
- External Service Network/Internal Management Network Boundary
- Internal Management Network/Secure Production Network Boundary
- Central Cloud/Station Boundary
- Boundaries Between Various Businesses
2. Cybersecurity Practices

2.7 Standards development

- IEC/TC9 is developing **IEC 63452 international standard** for railway cybersecurity, with 21 NCs including China, France, Japan.

- China is also developing **the railway cybersecurity standards** based on relevant laws and regulations, as well as horizontal standards.
PART 03

Proposals
3. Proposals

- Establish a cybersecurity framework oriented towards the rail transit industry in the Asia-Pacific region to meet various needs and scenarios
- Develop cybersecurity standards for the railway in the Asia-Pacific region
- Establish a cross-domain cybersecurity communication and cooperation platform in the Asia-Pacific region to enhance cybersecurity levels
Thanks, and best regards!

National Railway Administration of P. R. China