Railway Cybersecurity Challenges in South Korea
Cybersecurity Policies in South Korea

12 National Strategic Technologies (Presidential Advisory Council on Science & Technology)

- The designation of cybersecurity as a national strategic technology ('22.10, Presidential Advisory Council on Science & Technology Plenary Meeting)
  - Essential foundational technologies necessitated by the societal-wide digital transformation following the emergence of super-scale AI
  - The imperative need for top-level security systems and the fostering of strategic industries to maintain infrastructure and ensure national security

- Establishment of a cybersecurity strategic roadmap aimed at meticulously formulating and implementing mission-centric strategies to identify and secure core national technologies

- 4 key technologies: data and AI security, analysis and response in digital supply chains, network and cloud security, and industrial and convergence security

[Mission and Objectives of Cybersecurity Strategic Technology]
Cybersecurity Policies in South Korea

National Cybersecurity Strategy

• In response to increasing cyber threats such as hacking and information theft, the government has established the "National Cybersecurity Strategy" to ensure the safety and freedom of activities for our citizens in the cyberspace.
• Serving as the top-level guidance document in cybersecurity policy, the "National Cybersecurity Strategy" provides the national-level fundamental direction for enhancing capabilities to respond to cyber threats, fostering the information protection industry, and strengthening international cooperation in cybersecurity.

The Information and Communication Infrastructure Protection Act

• To ensure the safety of the nation and the stability of citizens' lives by establishing and implementing measures for the protection of key information and communication infrastructure against electronic intrusions, thereby ensuring the stable operation of such facilities in preparation for potential cyber threats.
Security Regulations for Government and Public Institutions

- **Security Compliance Verification System**: A system for verifying the security of information protection systems and network equipment introduced into government and public institutions. Through examinations based on the standards of the National Intelligence Service and the National Security Research Institute, this system aims to discover and address vulnerabilities that could lead to security incidents in advance, thereby enhancing the security level of information systems.

- **Cryptographic Module Verification System**: A system for verifying the safety and implementation suitability of cryptographic modules used to protect non-classified but important information communicated over the information and communication networks of government and public institutions.

Source: National Cybersecurity Center
Importance of Cybersecurity for Railway Signaling Systems

**Expansion of Adoption of Wireless Communication-based Train Control Systems**

- **Increased awareness and importance of security** due to the introduction of unmanned and automatic train operations in railways
- **Urban railway lines implemented with CBTC* (including KRTCS **)**

<table>
<thead>
<tr>
<th>Line</th>
<th>Train Control System</th>
<th>Date of Commissioning</th>
<th>Length(km)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sinbundang Line</td>
<td>Thales SelTrac</td>
<td>2011.10.28</td>
<td>33.5km</td>
</tr>
<tr>
<td>Busan Gimhae Light Rail Transit</td>
<td>Thales SelTrac</td>
<td>2011.09.16</td>
<td>23.4km</td>
</tr>
<tr>
<td>Incheon Subway Line 2</td>
<td>Thales SelTrac</td>
<td>2016.07.30</td>
<td>29.1km</td>
</tr>
<tr>
<td>Yongin Everline</td>
<td>Bombardier CITYFLO</td>
<td>2013.04.26</td>
<td>18.5km</td>
</tr>
<tr>
<td>Gimpo Gold Line</td>
<td>Nippon Signal SPARCS</td>
<td>2019.09.28</td>
<td>23.7km</td>
</tr>
<tr>
<td>Seoul Sinrim Line</td>
<td>LSE KRTCS</td>
<td>2022.05.28</td>
<td>7.53km</td>
</tr>
</tbody>
</table>

* CBTC: Communication-Based Train Control
** KRTCS: Korea Radio-based Train Control System
Importance of Cybersecurity for Railway Signaling Systems

Cybersecurity Technology Applied to CBTC

- **IPsec VPN**: Securing data protection and integrity by blocking unauthorized access
- **Limitations**
  - **Lack of device-level protection**: Current IPsec VPNs are only applied to the track-to-ground wireless network segment, failing to protect individual devices.
  - **Insufficient upper-layer protection**: Operating at the network's lower layer (Layer 3), IPsec VPN protects data at the packet level, unable to prevent forgery or manipulation of train control messages at higher layers.
  - **Inability for device authentication**: IPsec VPNs lack device-to-device authentication, requiring additional devices for multicast transmission.
  - **Absence of security features in trusted wired network**: Security features are not provided in a trusted wired network.
  - **Limitations of perimeter-based defense in trusted networks**: Once an attacker gains access, they can easily reach critical systems/data.
Importance of Cybersecurity for Railway Signaling Systems

Development of Railway Security Certification System (funded by MSIT)

• A system designed to enhance the security of CBTC by protecting train control messages (authentication, encryption, firewall, intrusion detection) at the network’s upper layer (Layer 7)

• Features
  - **End-to-end protection**: End-to-end protection of data transmitted between devices, not limited to wireless segments.
  - **Complete defense**: Operates at the network’s upper layer (Layer 7) compared to existing security methods (Layer 3), providing complete defense against cyber attacks.
  - **Mutual authentication**: Enables mutual authentication between devices and optimized for train control systems where availability is crucial, using lightweight authentication methods.
  - **Establishment of domestic TTA* standards**: Security requirements for wireless communication-based train control systems (TTAK.KO-12.0385)

* TTA: Telecommunication Technology Association
Challenges in Enhancing Railway Cybersecurity

Development of Railway Zero Trust Architecture to Counter Intelligent Cybersecurity Threats

- **Data/application security**: PKI (public key infrastructure)-based authentication
- **Micro-segmentation/SW defined perimeter**: dynamic network configuration
- **Integrated cyber-security policy management**: continuous monitoring through visibility

Example of Zero Trust remote exploitation scenarios

Source: NSA, “Embracing a Zero Trust Security Model”
Enhancement of Response to Digital Security Vulnerabilities and Collaboration Framework

- The establishment of a system to analyze and respond to digital security vulnerabilities is essential for protecting railway infrastructure and ensuring public safety amidst the digital transformation of railways.
- Given that cyber attacks on SOC could potentially escalate to the level of a national disaster, an integrated cyber security approach is needed across the entire lifecycle of railway components and systems to address advanced security threats.
Enhancement of Response to Digital Security Vulnerabilities and Collaboration Framework

• Strengthening the cybersecurity collaboration framework involves improving coordination and cooperation among stakeholders.

• This includes sharing cyber threat information and intelligence to respond to the latest threats, promoting the development of common cybersecurity standards and protocols, and fostering collaboration between government agencies, private sector entities, and international partners.

• By reinforcing collaboration, we can effectively address emerging cyber threats, share threat intelligence, and develop coordinated responses to cybersecurity incidents.
Thank you