深化亚太铁路运输数字化高级别会议

High-Level Meeting on Deepening Digitalization of International Rail Transport in Asia-Pacific

13 - 14 May 2025, Xi'an, China

Cybersecurity Threats and Countermeasures for China High-Speed Railway Network

SAIFEI Li

Southwest Jiaotong University, Chengdu, Sichuan



CONTENTS

1. China's High-Speed Rail Cybersecurity Threats and Challenges
2. Safeguarding High-Speed Rail Networks: China’s Practices
3. Summary and Prospects



China's High-Speed Rail Cybersecurity Threats and Challenges

Cyber threats: A never-ending challenge



The main arteries of national economic and transportation

Decrease in efficiency

Partial failure

Large-scale failure

Terrorist attack



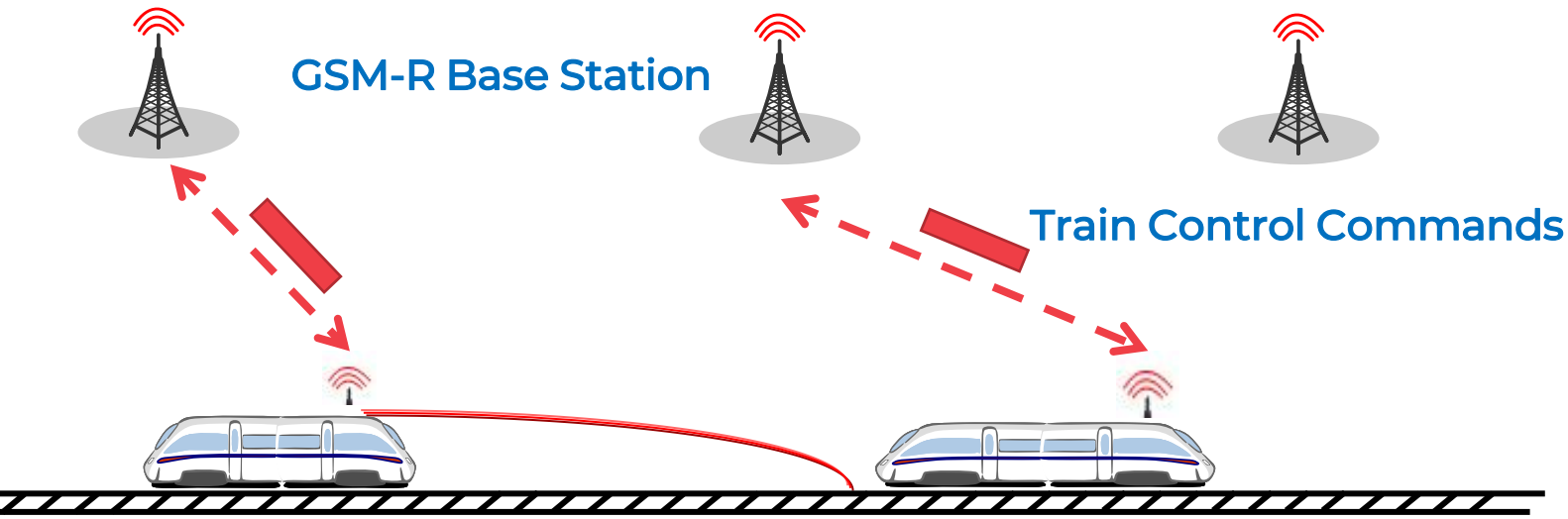






External Threats

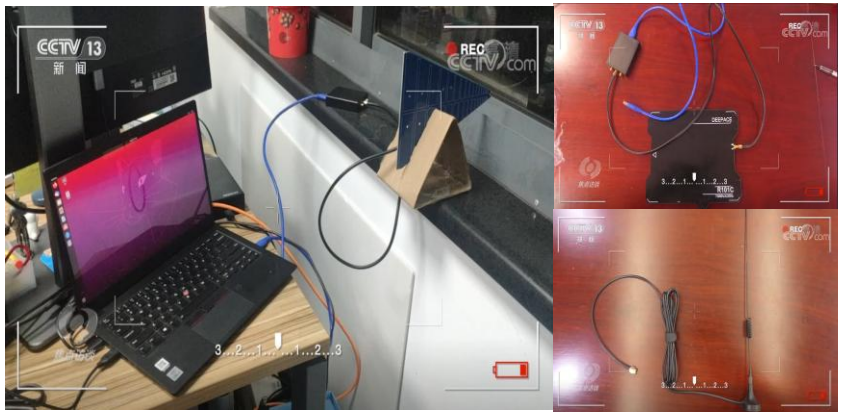
China's first high-speed railway data leak case cracked in 2022





Intercept GSM-R train-ground wireless communication signals

- **Phase 1:** Collect WIFI, 3G, 4G, 5G, and GSM-R signal data at specific locations.
- **Phase 2:** Conduct mobile testing and data collection in 16 cities (including Beijing and Shanghai) and along corresponding high-speed rail lines.



Captured data interception equipment

Internal Challenges

☐ Challenge 1: Special Requirements for Security Protection of Railway Safety-Critical Systems

01 Safety

- ☐ Security measures must not disrupt control processes
- ☐ Any added security software /hardware must comply with the Safety Integrity Level(SIL)

02 Real Time

- ☐ Security measures must meet real-time communication requirements and support diverse protocols.
- ☐ High-priority control data bypass security layers

03 Maintainability

- ☐ Lifecycle Mismatch: device lifecycles of 15-20 years
- ☐ System patches or security updates may disrupt the deterministic behavior of safety-critical software

Contrary to conventional IT practices (firewalls, intrusion detection, malware removal), railway systems demand integration of security and safety by-design approaches.

Internal Challenges

☐ Challenge 2: Cybersecurity Risks from Emerging Technologies in HSR.

Expanded Attack Surface

- ☐ Cloud computing, big data, 5G, IoT, satellite positioning， navigation, and AI
- ☐ Novel attack vectors targeting newly digitized components
- ☐ Vulnerabilities concealed in closed environments are exposed in open architectures

Siloed Safety-Security Design Paradigm

- ☐ Current practices treat safety and security as isolated domains
- ☐ Fail to identify conflicts between safety and security objectives at early design stages
- ☐ Result in unmitigated operational risks during system deployment.

Escalating Supply Chain Threats

- ☐ Undocumented backdoors and logic flaws in critical components
- ☐ Third-party risks from multi-vendor technology stacks

Internal Challenges

☐ Challenge 3: Railway Workforce Lack Security Awareness/Competency.

Foundational Knowledge Gaps

- Operational workflows remain decoupled from cybersecurity contexts
- The latest security technologies for rail networks have not been updated among staff.

Inadequate Security Analytics

- Ineffective analysis capabilities against novel cyberattacks.
- Inability to address unknown and sophisticated threats.

Reactive Risk Anticipation

- Incident response over proactive defense
- Insufficient mechanisms for predictive risk modeling to counter rapidly evolving threat landscapes

Improper Response

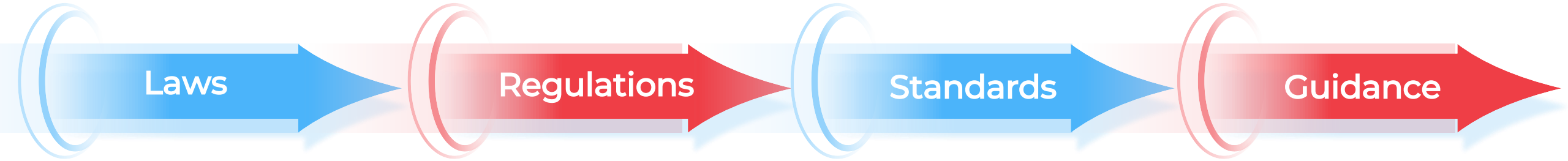
- The railway security incident response framework requires further enhancement.
- Ineffective and improper handling of emerging security incidents persists.



Safeguarding High-Speed Rail Networks: China's Practices

- Cybersecurity Governance Framework
- Cybersecurity Defense Architecture

Cybersecurity Governance Framework for Railway



- Cybersecurity Law
- Data Security Law
- Cryptography Law

- Regulations on the Security Protection of Critical Information Infrastructure
- Regulations on the Multi-Level Protection Scheme (MLPS) for Cybersecurity

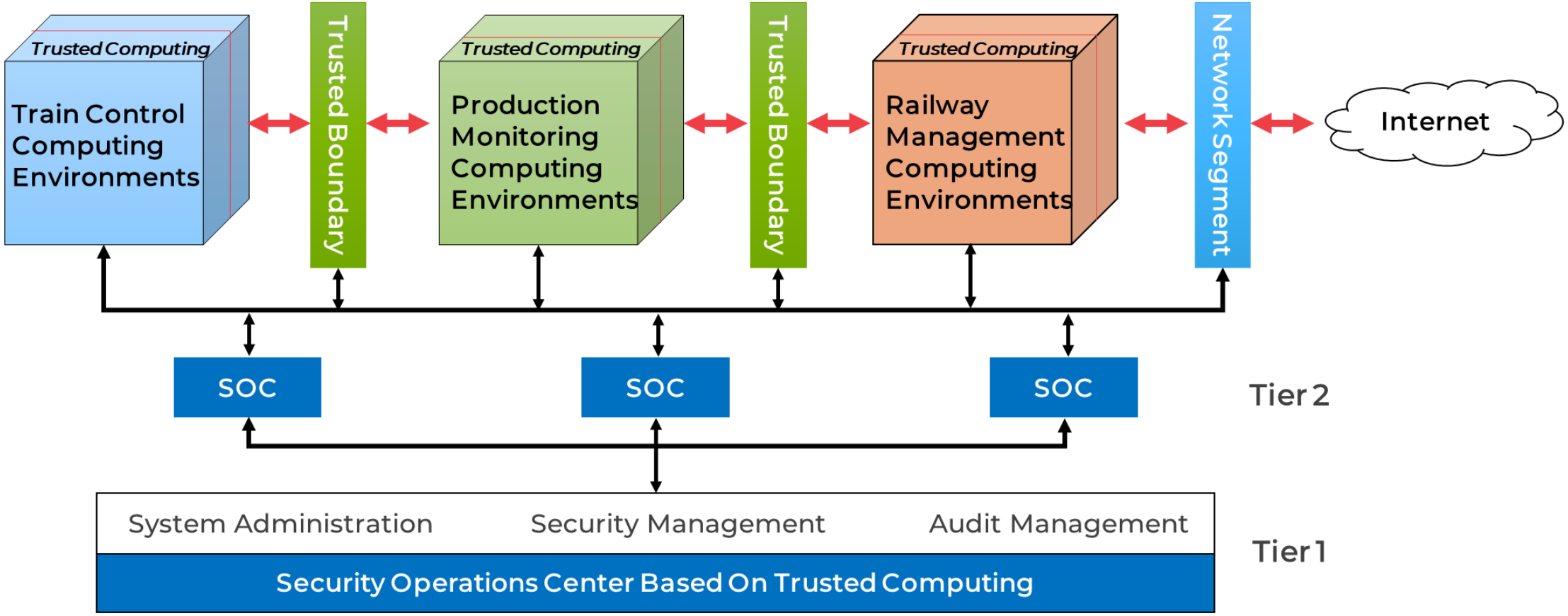
- Security Protection Requirements for Critical Information Infrastructure (CII)
- Basic Requirements for Railway Cybersecurity Multi-Level Protection

- Administrative Measures for the Security Protection of Railway Critical Information Infrastructure
- Risk Assessment Specifications for Railway Critical Information Infrastructure

China Cybersecurity Law:

- **Article 21:** The State Implements a Cybersecurity Multi-level Protection Scheme (MLPS).
- **Article 31:** The State implements enhanced protection for critical infrastructure in vital industries and fields on the basis of the MLPS.

Cybersecurity Defense Architecture for Railway



Achieves Three Assurance Objectives:

- Trustworthiness: Via cryptographic chaining from hardware to application layers.
- Controllability: Implementing that subjects (users) access objects (information resources) according to policy rules.
- Manageability: Enabled by SMC's centralized management with the separation of powers among System Administration, Security Management, and Audit Management.



Summary and Prospects

Lessons Learned and Future Directions

01. Lessons Learned

- ***Regulatory and Standardization :*** China's HSR cybersecurity framework operates under a unified regulatory ecosystem. Centralized governance and interagency coordination enhance systemic accountability.
- ***Human-Centric Risk Management :*** Human factors remain the weakest link; Continuous training and behavioral safeguards are critical.
- ***Innovation in Emerging Technologies:*** Proactive investment in next-gen technologies future-proofs infrastructure against sophisticated threats.

02. Future Directions

- ***Integration of Security and Safety by-Design:*** Security and Safety integration during the design phase reduces long-term risks from the source.
- ***Expand global cybersecurity alliances :*** Recommend to establish a multilateral platform for sharing threat intelligence and joint response protocols against attacks on critical railway infrastructure.

Thanks for your attention.

SAIFEI Li

Southwest Jiaotong University

Email: lisaifei@swjtu.edu.cn

