Draft Regional Framework on Strengthening Rail Cybersecurity in Asia-Pacific

Sandeep Raj Jain
Transport
Division

ESCAP
Economic and Social Commission for Asia and the Pacific

Outline

- Background
- Challenges to rail cybersecurity
- Key recommended actions



Background



- ✓Strategy 2030 on Accelerating Rail Digital Transformation in Asia-Pacific provides for rail cybersecurity as one of the enablers and recommends developing a regional framework to strengthen rail cybersecurity

- ✓Growing digitalization and artificial intelligence capabilities, no doubt increase efficiency and reduce costs however they would expose rail systems to cyber threats.

- ✓Growing rail cyberattacks in the form of ransomware, malware, data breaches, supply chain weaknesses can lead to disruption of services with attendant economic and other losses, damage to rail infrastructure and at worse loss of lives.

Challenges for rail cybersecurity



- ✓Longevity and legacy of rail assets
- ✓Prevalence of wide range of stakeholders
- ✓Analyzing rail safety due to cyber threats
- ✓Wide geographical spread of rail assets
- ✓Low capacity of rail officials
- ✓Financing constraints

Key actions for enhancing rail cybersecurity

1. Develop a comprehensive policy for rail cybersecurity that is aligned to national cybersecurity policy



- ✓Rail should be part of critical national infrastructure
- ✓Comprehensive understanding of rail digital ecosystem including *inventory digital assets* and cyber-interfaces and a *risk-based approach* to secure to manage cyber threats
- ✓ The policy should include means to
  - secure OT and IT systems and interfaces
  - data protection and procurement policy
  - incident response and recovery
  - governance structure
- ✓Methodology to undertake rail cybersecurity assessment for countries

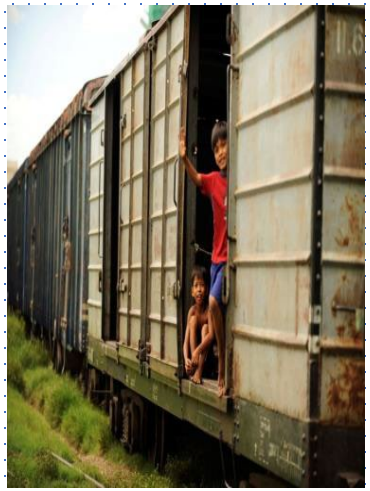
2. Consider developing subregional/regional standards/regulations on rail cybersecurity

- Unique rail environment in Asia-Pacific characterized by existence of
  - ✓Different rail gauges, rolling stock and operational practices
  - ✓Integrated infrastructure and operations; and
  - ✓Three types of rail, namely, high-speed and highly digitalized, digital metro systems and traditional heavy rail used for freight and passenger

- Globally several regulations/standards have been developed on rail cybersecurity
  - ✓European Union Network and Information Systems (NIS) Directive
  - ✓European Union General Data Protection Regulation (GDPR)
  - ✓IEC 62443 suite of standards for cyber security of industrial automation
  - ✓CENELEC 50701 technical standard for railway cybersecurity
  - ✓UIC Guidelines for Cyber-Security in Railways

Key actions for enhancing rail cybersecurity

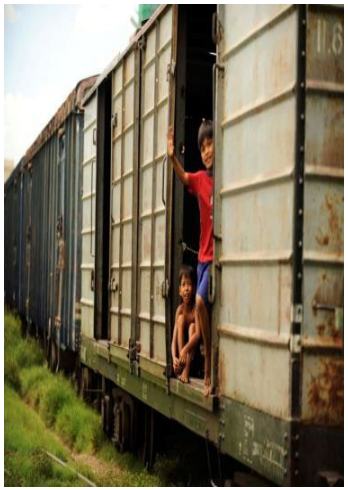
2. Consider developing subregional/regional standards/regulations on rail cybersecurity



- ✓None of the existing standards/regulations address all aspects of rail cybersecurity
- ✓It appears countries in the region have different approaches on rail cybersecurity
- ✓Consider developing subregional standards or regulations or principles to reduce fragmentation and compliance challenges
- ✓Constitute a *group of experts* from interested countries to consider this and present recommendations at the Working Group

Key actions for enhancing rail cybersecurity

3. Enhance capacity for rail cybersecurity



- ✓With digitalization, apart from traditional skills, *digital competencies and capabilities* are essential for operation and maintenance
- ✓Skills are needed to understand, advise and quantify *cyber risks* to stakeholders in an organization
- ✓A *cyber security culture* needs to be developed -where in a digital ecosystem any erroneous events are reviewed and across an organization the role of cyber security
- ✓Upskilling the workforce with strong cyber security capability can require *significant investment and time*
- ✓Develop a dedicated regional capacity building programme on rail cybersecurity

Key actions for enhancing rail cybersecurity

4.Establish regional rail cybersecurity task force



Establishing collaborations between member states can provide significant opportunities and mutual benefits on addressing rail cybersecurity threats

- Information sharing – sharing relevant information about emergent cyber security threats, indicators of compromise/attack, and threat intelligence which other member states who may not possess or have access to
- Knowledge exchange – to promote mutual development of knowledge, skills, and expertise

Key actions for enhancing rail cybersecurity

4. Establish regional rail cybersecurity task force



- Identifying and resolving shared issues – a specific challenge in railway cyber security within one member state may be shared by other states. Each bringing their knowledge, expertise, and insight to address them

- It is suggested to establish a **regional rail cybersecurity task force** which can also serve as a regional information exchange mechanism on rail cybersecurity to address the common challenges

Key actions for enhancing rail cybersecurity

5. Engage public private partnership to foster innovation and reduce costs



- Private sector have significant rail cybersecurity experience and therefore it is critical to engage them throughout the lifecycle of rail assets
- Ensure that the common approaches to cybersecurity requirements developed at a regional, sub-regional level and at national level are agreed by end users and suppliers
- Suppliers can develop product roadmaps and solutions early to meet these requirements, rather than on a per-project basis leading to *economies of scale*

Next Step



Finalized Regional Rail Cybersecurity Framework is being put up for adoption at the Working Group on Trans-Asian Railway at its 9th Meeting to be held in September 2025 in Bangkok

Thank you
for
your attention

http://www.unescap.org/our-work/transport

