Session 2: Railway Cybersecurity

Rapporteur: Felicita Di Giandomenico

Presenters:

Francesco Brancati, ResilTech S.r.l.

Andreas Polze, Hasso-Plattner-Institut, Universität Potsdam

88th IFIP Meeting, Ischia, 29 June 2025

Current challenges in applying cyber-security in railway signalling systems according to current available cyber-security standards

- A critical perspective on how cybersecurity is currently applied in the railway sector
  - with a specific focus on the practical challenges of adopting the IEC 62443 standard and the CLC/TS 50701 technical specification

- Key implementation gaps affecting today's projects:
  - Tendency to assign flat Security Level Targets per zone, regardless of functional roles and exposure
  - Overdesign risks due to a lack of guidance on SL-T assignment
  - Incompatibility between generic SL-T targets and railway-specific constraints (e.g. well-established safety processes and standards)

- Through concrete examples (DMI, OTM, JRU), the presentation showed how inappropriate SL-T assignments can lead to unrealistic requirements or ineffective protections

- A context-aware methodology is introduced as a practical solution to assign a tailored SL-T value for each node in a zone (based on real exposure and functional impact), that applies:
- Node-level threat modeling using STRIDE-LM
- Risk estimation through an Attack Feasibility Rating (AFR)
- Generation of SL-T vectors per Foundational Requirement (FR)

The final message is that SL-T must not be treated as a fixed label, but rather as the result of a documented, reasoned, and reproducible process, aligned with both risk and architectural constraints

Digital Railway Operation - CyberSecurity in Critical Infrastructures

- Covered many aspects around the digital railway operation, including:
  - The EULYNX Initiative:
    - Defining an internationally standardised signalling system
    - Focus on modular signalling architecture with common standardised interfaces
    - Standing organisation for continuous development, maintenance and change management of the standards
    - Support the certification of products
    - Support infrastructure managers in the implementation of the standards

  - ENISA report - Security measures in the Railway Transport Sector

  Cybersecurity Challenges:
    - Low digital and cybersecurity awareness in the railway sector
    - Difficulty in reconciling safety and cybersecurity worlds
    - Digital transformation of railway core business
    - Dependence on the supply chain for cybersecurity
    - Geographic spread of railway infrastructure and the existence of legacy systems
    - The need to balance security, competitiveness and operational efficiency
    - Complexity of regulations for cybersecurity

Final considerations:

Digitalization is going to weaken Command Control and Signalling for railway systems

- Need to cope with long system lifetime (…multiple decades)
- Innovative technologies are prone to attacks
- Certification processes need to be adapted
- SW-based CCS for railway needs to be certifiable and updatable at a low cost
- Fail-stop vs fail-operational: trading off safety and availability
- Attention to threats arising from publicly available confidential data about the infrastructure
- Resiliency needs to be considered separately

Physical Security of digital CCS for railways today is of much bigger concern than CyberSecurity