Cybersecurity for Rail: constraint or opportunity?

Thomas CHATELET
ERTMS Project Officer / EU Agency for Railways
Cybersecurity for Rail: a reality?
### Shared roles and responsibilities

#### Operational Control and Maintenance
- Traffic Management System
- Communication (Train Driver Trackworker)
- Maintenance Management and Diagnostics
- Network Management System
- Energy Management System
- Facility Management (Power, AirCon, Supervision etc.)
- Passenger Information System (PIS)

#### Infrastructure
- Interlocking
- Electrical Substation
- Tunnels (e.g. STES)
- Bridges
- Diagnostics
- Digital Signage
- Entertainment (e.g. WiFi, Internet)
- Radio Block Center
- Communications (e.g. GSM-R MSCU BSC)
- CCTV (Video Surveillance)
- PA (Public Address)
- PIS (Passenger Info System)

#### Trackside
- ATP (Railsea, Loop)
- Point Machine
- Level Crossing
- Signal
- Train Detection Sensor

#### On-board
- ATP (Automatic Train Protection)
- Fire detection and extinguisher
- TCMS (Train Control Monmg. System)
- TCN (Train Control Network)
- Diagnostics
- HVAC
- Entertainment (e.g. WiFi, Internet)
- PAS (Passenger Alarm System)
- Driver/Attendant Interface
- Cab Radio
- Anti-intrusion
- PA (Public Address)
- Event Recording
- Driver Advisory System
- EMS (Energy Metering System)

#### Colour Legend
- Signalling
- C2M & Control
- Auxiliary
- Comfort
- Public

---

From draft TS 50701
Railway related cybersecurity initiatives

• TC9X - Working Group 26
  • Draft Technical specification 50701: “Railway Applications – Cybersecurity”
    ➢ Consistent approach to introduce requirements and recommendations for cybersecurity within the railway sector

• Technical Committee CYBER
    ➢ Guidance on considerations for incident notification; best practices in cyber security risk management

• Technical Demonstrator 2.11
  • Definition of a security by design system, dedicated to railways (e.g. Protection Profiles Specification)
    ➢ Application of the methodology to railways (demonstrator)
Railway related cybersecurity initiatives

• Cyber Security Solutions Platform
  • Practical solutions for cybersecurity, from a telecom angle, focusing on critical elements of the railway system

• ER-ISAC
  • European Rail – Information Sharing and Analysis Centre
  • Circa. 50 members under the lead of IMs/RUs (FR/DE/BE/NL)
    ➢ Share best practices, discuss common vulnerabilities, influence regulation and standardisation
ERTMS & Cybersecurity

• Need to improve ERTMS robustness against cyber threats
  • ETCS
    ➢ More robust algorithm to replace 3-DES
    ➢ E2E authentication mechanisms for EVC-RBC communication
    ➢ Operational measures (e.g. online key management)
  • GSM-R
    ➢ Systematic encryption of the air interface
    ➢ Monitoring tools to spot abnormal operation
  • FRMCS
    ➢ Security by design requirements to be inserted in FRMCS specifications
• Need to take into consideration Operational harmonisation
Cybersecurity @ ERA

**Regulation considerations**
- Monitor relevant activities related to cybersecurity in the railway context
- Cover safety requirements of the rail system, e.g. the assessment of safety consequences originated by cybersecurity threats
- Reflect the above in Technical Specifications for Interoperability and Common Safety Methods

**Cooperation building**
- Close relationship with ENISA and European Commission in support of railway stakeholders
- Cross-fertilisation with EASA and EMSA to develop a transport cybersecurity policy
- Review with National Cybersecurity Agencies (e.g. ANSSI, BSI) potential gaps
- Support ER-ISAC
Thank you! for your kind attention