Cybersecurity in Railways
ERA-ENISA webinar
ERA activities on cybersecurity

EUROPEAN UNION AGENCY FOR RAILWAYS

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

Cybersecurity for Rail: new opportunities / novel challenges

ERA Cyber activities 1/2

- To **monitor** all activities related to cybersecurity in the railway context
  - Identify and promote adoption of security-by-design features in **future radio communication and signaling systems**
- To cover safety requirements of the rail system, including the assessment of **safety consequences originated by security threats**
  - Security threats based on physical access to assets outside of scope
  - Digital inherent threats considered
  - Safety AND Security Management Systems
- To reflect the above as necessary in the EU railway regulation
  - **TSIs** (TAF/TAP, OPE, CCS) : technical requirements to guarantee interoperability, e.g. increase the cyber robustness of ERTMS
  - **CSMs** : process oriented requirements to guide the acknowledgement of cybersecurity issues that might influence safety

Relevant railway cybersecurity initiatives

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

contact@er-isac.eu

TC9X - Working Group 26

- Draft TS 50701: "*Railway Applications – Cybersecurity*"

  → Consistent approach to introduce requirements and recommendations for cybersecurity within the railway sector

Relevant railway cybersecurity initiatives

IP2 - Technical Demonstrator 2.11

- Definition of a security by design system, dedicated to railways (e.g. Shared Security Services, Protection Profiles Specification)

  → Application of the methodology to railways (demonstrator)

Cyber Security Solutions Platform

- Practical solutions for cybersecurity, from a telecom angle, focusing on critical elements of the railway system

Relevant railway cybersecurity initiatives

ENISA

- TRANSSEC - Transport Resilience and Security Expert Group

→ Forum on specialised work streams to exchange viewpoints and ideas on cyber security threats, challenges and solutions
(Air / Rail / Water / Maritime Transport)

DG MOVE

- Transport Cybersecurity Toolkit

→ Study on the main cybersecurity threats, potential consequences, and risk mitigation actions for transport companies

Technical Committee CYBER

- Technical Report: "*Implementation of the NIS Directive*"

→ Guidance on considerations for incident notification; best practices in cyber security risk management

EUROPEAN UNION AGENCY FOR RAILWAYS

ERA Cyber activities 2/2

- To foster **close cooperation with ENISA and EC**
  - Support railway stakeholders on cybersecurity strategy development
  - Consider incident reporting schemes
- To cooperate with **EU-Agencies in the transport sector (EASA, EMSA)**
- To dialog with **National Authorities** on potential gaps in cybersecurity requirements
  - Cybersecurity Agencies (e.g. ANSSI, BSI…)
  - Railway Safety Authorities (e.g. Traficom, EPSF…)
- To support the **ER-ISAC** (European Rail-Information Sharing & Analysis Center), and consider their deliverables in the evolution of the rail regulatory framework

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** on transport cybersecurity policy
- Dialog with **National Authorities** on potential gaps
- Support **ER-ISAC**

EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Follow us on ERA_railways

Discover our job opportunities on **era.europa.eu**

ISO 9001:2015
BUREAU VERITAS
Certification