Cyber Security and Regulation in Rail

CyberSecurity for Rail, Brussels, 4 October 2017
Josef Doppelbauer, Executive Director
The Single European Railway Area

Make rail more competitive
+ Market opening
+ International operation
+ Interoperability
+ Safety

safe :: connected :: affordable
Data Enabled Railway Operation

- **Rail has to innovate**, responding to new demands of customers regarding mobility and logistics
- **Digital technology** can be a disruptive innovation in all areas of the railways, also helping to integrate transport modes (seamless multi/modal transport)

... applied to processes across the entire value chain (passengers and freight)
Digital Railways in Europe

(All) European railway undertakings invest heavily in digitalization

The focus is on company use and not on a wider strategic agenda
There is a Data Interoperability Problem

**GOAL:** Multimodal Stakeholders with their own proprietary data sets exchanging information in a seamless manner

(ERA internal lack of data interoperability is just an instantiation of a generalized data interoperability problem in the multimodal transport data context)
What can the actors in the railway sector do, in order to protect themselves, their services, and their customers from Cybercrime?
The EU Cyber Policy

In order to scale up the EU’s response to cyber-attacks, to improve cyber resilience, and to increase trust in the Digital Single Market, the European Commission has proposed:

• The European Agency for Network and Information Security (ENISA, established in 2004) is proposed to become the European Union Cybersecurity Agency, with a permanent mandate to assist Member States in effectively preventing and responding to cyber-attacks, as well as increased resources.

• The establishment of an EU cybersecurity certification framework that will ensure the trustworthiness of the billions of devices (“Internet of Things”) which drive today’s critical infrastructures, such as energy and transport networks, and also new consumer devices, such as connected cars.
EU-Wide Regulation – the NIS Directive

- Obligations for all Member States to adopt a national Network and Information Systems (NIS) strategy and to designate National Authorities
- Obliges Member States to designate national competent authorities and CSIRTs*
- Creates first EU cooperation group on NIS, from all Member States
- Creates an EU national CSIRTs network
- Establishes security and notification requirements for operators of Essential Services (ESP) and Digital Service Providers (DSP)

* Computer Security Incident Response Team
IT Security Activities Related to Railways

• **CENELEC: SG 16 → SG 24 → New WG 26 (to be started soon)**
  → Implementation of a consistent approach to the management of the security of the railway systems

• **ETSI: TC CYBER**
  → Guidance on considerations for incident notification; best practices in cyber security risk management

• **Shift²Rail: TD 2.11**
  – Definition of a security by design system, dedicated to railways
  – Application of the methodology to railways (demonstrator)
Railways Need to Protect Their Systems and Data

... in a collaborative manner

(resilience stands and falls with the weakest component)
The EU Agency for Railways Action Plan

• To monitor all activities related to cybersecurity in the railway context
  – Promote adoption of native security 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
  – Threats inherent in the radio link considered
  – Safety AND Security Management Systems
• To reflect the above in TSIs (TAF/TAP, OPE, CCS) and CSMs
• To foster close cooperation with ENISA and EC
  – Support railway stakeholders on cybersecurity strategy development
  – Assist the development of network of Railway Cyber Security Experts
  – Consider incident reporting schemes
• To cooperate with other EU-Agencies in the transport sector (EASA, EMSA)
• To support the concept of an ISAC (Information Sharing & Analysis Center) for Rail
The Dark Side is Constantly Finding New Ways to Break Security

By failing to prepare, you prepare to fail!
Making the railway system work better for society.

Follow us on Twitter: @ERA_railways