DB NETZE INFRABEL Right On Track SNCF RÉSEAU ProRail

ER-ISAC

European collaboration in the field of CyberSecurity for Railways - Inspiration for Inland Navigation?

Workshop on cybersecurity in Inland Navigation

ER-ISAC | Christian Schlehuber (Co-Chair) | Bonn | 2019-09-05

Introduction to Railway Systems

Biggest business premise in Europe – **with public access**

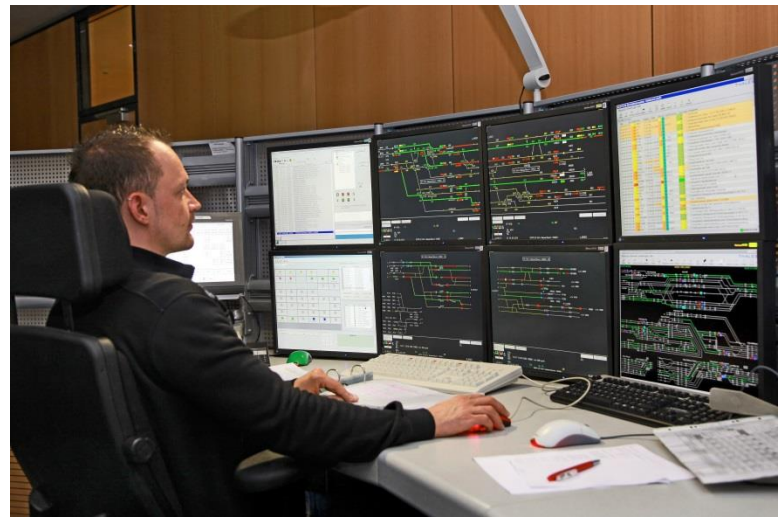
- Stations as gate to railway transportation
- Europe-wide rail networks

Strong regulations of technical installations (according Safety)

- EN 50126 (Reliability, Availability, Maintainability, Safety – RAMS)
- EN 50128 (Software for safety systems)
- EN 50159 (Communication)
- Etc.

➔ National Safety Authority has to grant **admission for every interlocking**

➔ Categorized as **Critical Infrastructures** in most European countries



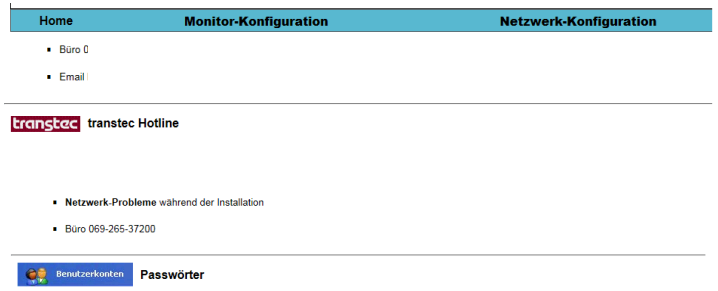
Threat Landscape in the Railway Domain

ER-ISAC

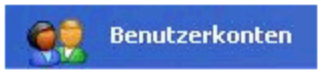
- Railway technologies are sector specific and split into **Signaling, Rolling Stock and Fixed Installations**
- Systems have a **lifetime of 30+ years**
- **Digitalization** initiatives move Infrastructure towards intelligent, more connected, more assisted systems
- **Obsolescence** of Safety systems exposed to current and future cyber threats landscape
- **Standards** for Railways currently **not up to date with CyberSecurity** challenges
- **Awareness** not at a desired level

Security Controls vs. Reality

Security Controls vs. Reality



- **Netzwerk-Probleme** während der Installation
- Büro 069-265-37200

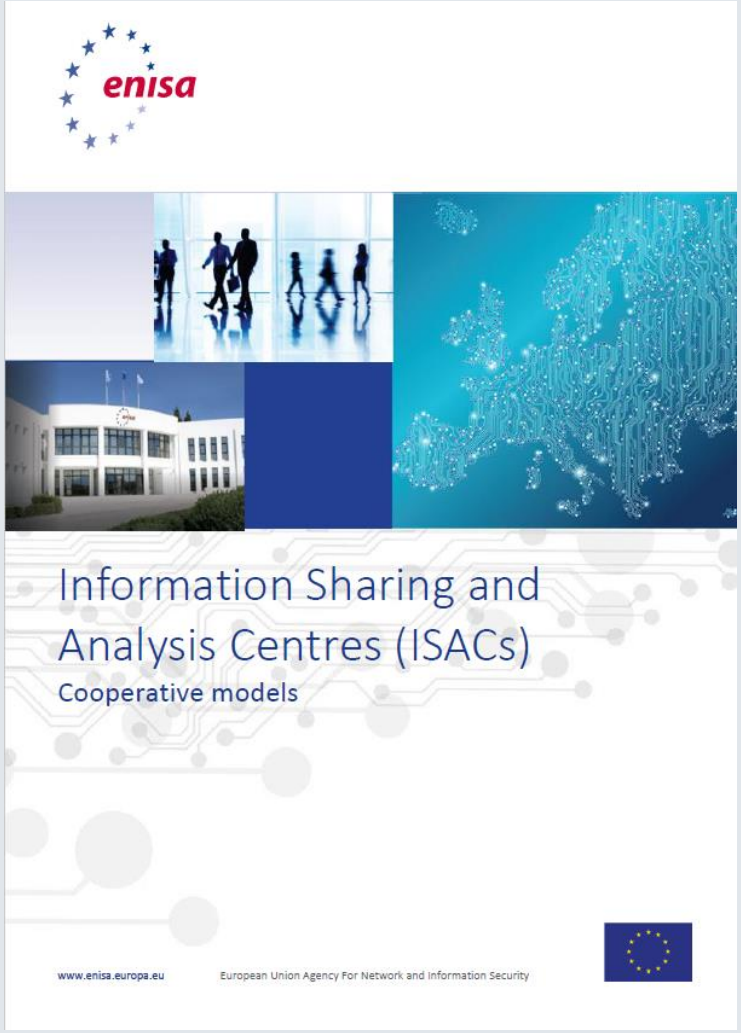


Passwörter

- **Benutzer** : disponent **Kennwort** :disponent
- **Benutzer** : administrator **Kennwort** : bundesbahn

The role of ISACs in Europe

- **Information Sharing and Analysis Centres (ISACs)** required by European CyberSecurity Act
- **Non-profit organizations** that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure)
- Allow **two-way sharing of information** between the private and the public sector
- ISACs create a platform for such cooperation in term of sharing information about root causes, incidents and threats, as well as sharing experience, knowledge and analysis
- Further information can be found in the report by ENISA: *https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models*



Members per Countries (Sept 2019)

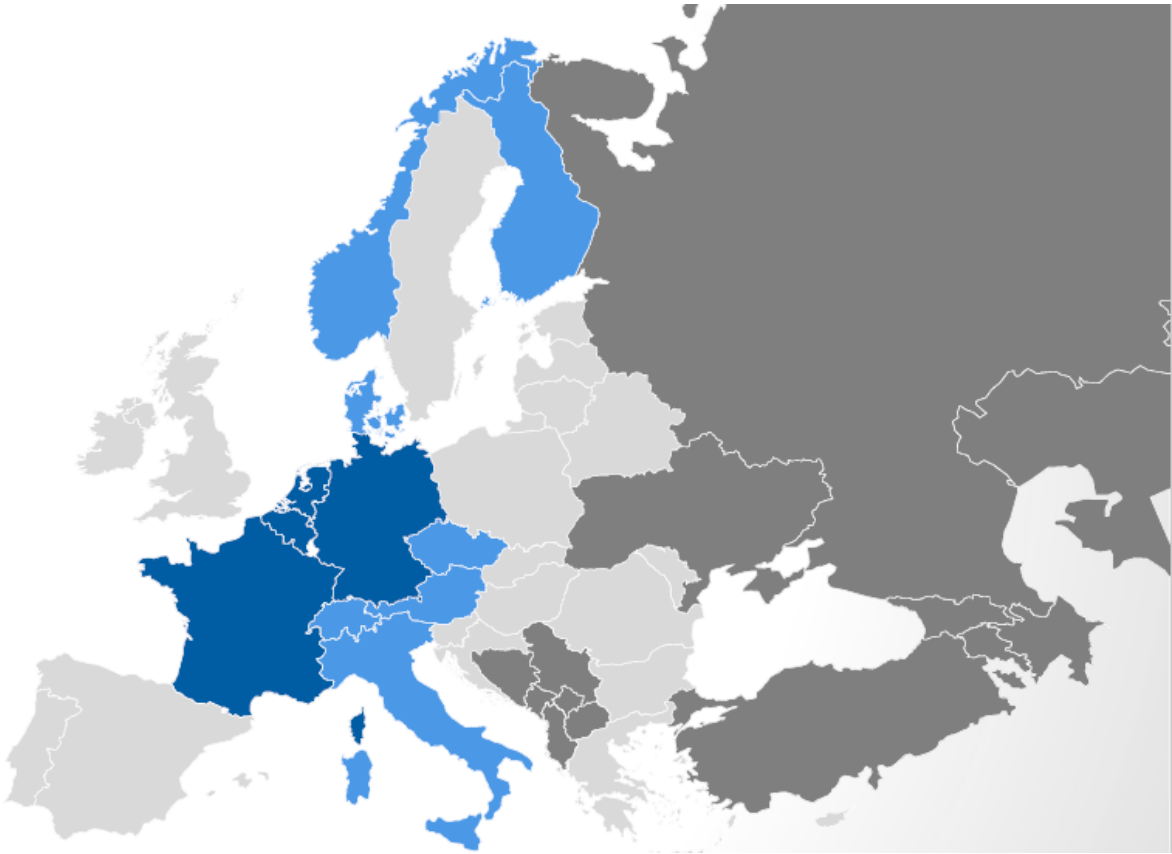
Already 50 organizations taking part since ER-ISAC Kick-Off end of 2018

Co Chair
FR /DE /BE /NL

Members
FI /NO /DK /IT /CH /AT /CZ

Members to be contacted

Possible future partnership



Why collaborate in CyberSecurity in the Railway?

- Standardization of technologies used across Countries (even outside EU = ERTMS)
- Specific technologies for Signaling systems and Rolling Stock
- Same supply chain
- Specific Standardization for Safety in the Railway

➔ **The same issue affects us all**

How will we benefit from the ER-ISAC – Our Vision

ER-ISAC

- Experiences in how aspects of cyber security are handled
  - CyberSOC, ICS, IoT, Artificial Intelligence usage, Crisis management, …
- Cybersecurity standards for Safety related products
- Cybersecurity products certifications and experience
- Alerts/ early warnings, Threat intel, experiences on products vulnerabilities specific to Railway, References on a wider range than national
- Meet regularly to discuss and share information (e.g. threat landscape, fact based approached, …)
- Security Supply chain management (same level of security MUST BE delivered across European Railway by same provider)

Collaboration on CyberSecurity Standardization

CENELEC TC 9X – WG 26 (CyberSecurity)

- Working Group on “Railway Applications – Cybersecurity”
  - Covers Signalling, Rolling Stock, Fixed Installation
  - Started November 2017
- 72 experts (20-30 experts participating to F2F meetings; approx. 6-10 meetings per year)
- Experts from 12 countries (+ ERA and ENISA as observer)

Goal:

- Establish a TS (prTS 50701) for handling CyberSecurity in a unified way for the whole railway sector
- Based on already existing IT-Security standards (e.g. IEC 62443)

Status:

- Enquiry phase finished with ~2200 comments from NCs; TS to be finalized till mid 2020

Collaboration on CyberSecurity Standardization

ER-ISAC

How can the Inland Navigation benefit from cooperation

ER-ISAC

Assumed challenges:

- Finding technical expertise in CyberSecurity
- Not enough resources & funding (expertise, tools, personnel)
- Suppliers not always cooperative

The Strength of Unity as a Sector:

- Creation of expert groups from suppliers, industry and CyberSecurity providers **(Threat Intelligence)**
- Gather actors on board to lobby International Authorities to adapt Regulations **(Compliance)**
- Create communication bridges between operators and infrastructure managers CSIRTs for rapid intervention with experts to assist **(Incident Response)**
- Assess and create minimum security baseline to enforce it into supply chain **(Cybersecurity by design)**
- Integrate R&D innovation projects as a governance body / testing body **(Continuous protection)**
- Involve Locals Governments CSIRT's to assist in cross borders risks **(Cyber resilience)**

Thank you for your attention

M.Sc. Christian Schlehuber
Lead of CyberSecurity R&D

DB Netz AG
I.NVI 1(S)
Weilburger Str. 22
60326 Frankfurt am Main

Phone: +49 152 3753 7938
christian.schlehuber@deutschebahn.com
contact@er-isac.eu
www.er-isac.eu

http://www.er-isac.eu