Forum on Sustainable Transport Connectivity between Europe and Asia

Olivier De Visscher, Chairman of the European Rail Information Sharing and Analysis Center (ER-ISAC), Belgium
Thomas Faenoe, Chief Information Officer, Rail Net Denmark
ER-ISAC contributes to the forum on security aspects of integrated intermodal transport and logistics. ER-ISAC provides an inclusive platform for railway undertakings in the EU to collectively exchange information on and tackle cyber security threats.

Those threats are explained on the next slides.
European Rail Information Sharing and Analysis Center (ER-ISAC)

Presented by:
Olivier de Visscher ER-ISAC Chairman

With assistance of:
Thomas Faenoe from Railnet Danmark

and contribution from:
Dr Jasmin Cosic from DBNetze Germany

Reach us at: Contact@ER-ISAC.EU
The threat landscape in the Railway transport sector

- Railways technologies are sector specific and split into Signalling and traffic management systems;
- Most of them are safety related systems: Interlocking systems, Speed control, traffic management, Automatic driving, SCADA, remote monitoring and supervision, GSM-R, ETCS-L2, …
- Infrastructure Railway Managers or Railway Undertakings (Operators) are using the same technologies and methods across countries;
- Infrastructure moves towards intelligent, more connected, more assisted systems;
- More data exchange between sectors (Airports, Harbours, …);
- Obsolescence of Safety systems exposed to current and future cyber threats landscape;
- Standards for Safety in Railway not up to date with current cybersecurity challenges
Digitisation of Trains introduces cyber risks

- Datacentres on Wheels
- Publicly accessible, Valuable customer info
- Digitisation of Safety control system (ERTMS)
- Cyber securing Operational systems
- IOT
- RTM
- Predictive Maintenance
There is a great need for policy and oversight.

Rail Industry cyber risk control is immature

Threats sophistication increases threat surface = increase incidents

Critical Infrastrucure? Regulation Standardisation

Actually happened

- Dublin’s Luas tram system Website hacked
  - January 2019
- Indian Railway Catering and Tourism Corporation hacked
  - 2019
- Hackers access accounts of 1,000 Great Western Railway customers
  - April 2016
- WannaCry attacks,
  - Deutsche Bahn, ticketing and information systems
  - Germany’s rail network
  - May 2017
- Four cyber attacks on Uk Railways
  - July 2016
- Chaos Computer Club, 32nd congress, Hamburg, December 27, 2015

Hypothetically possible

NON DISCLOSED

- Four cyber attacks on Uk Railways
  - July 2016

Actually happened

- Hackers access accounts of 1,000 Great Western Railway customers
  - April 2016
- WannaCry attacks,
  - Deutsche Bahn, ticketing and information systems
  - Germany’s rail network
  - May 2017
- Four cyber attacks on Uk Railways
  - July 2016
- Chaos Computer Club, 32nd congress, Hamburg, December 27, 2015

NON DISCLOSED
The role of ISACs in Europe – and in particular with regard to developing measures to counter cyber threats to (rail) transport networks at the cross border level

Information Sharing and Analysis Centres (ISACs) are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector. ISACs have created communities within the private sector. They could be oriented on a specific critical sector (e.g. finance, energy, health) or serve as a focal point on the national level to gather information about cyber incidents and analyse it.

To ensure the right level of cybersecurity, cooperation between the public and the private sector is absolutely crucial. 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. In Europe, the first ISACs focused on the Finance and Energy sector.

ER - ISAC

Members per Countries (Oct 2019)

54 organisations since foundation on 4th of June 2019

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?

Standardisation of technologies used across Countries (even outside EU = ERTMS)

Specific technologies for Signalling systems

Same supply chain

Specific Standardisation for Safety in the Railway

=> One issue affects us All
How will the EU Railway Cybersecurity Platform (ISAC) help us

Our vision for collaboration

- 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)
Trust building by non competitive environment

► Important to be able to share information only among Rail Infrastructure Managers and Railway Undertakings
  ► Plenary sessions with all parties involved
  ► Dedicated discussions in working groups as relevant

- Discuss Common Vulnerabilities (e.g. ICS)
- Share Best Practices (e.g. CyberSOC)
- Industry Challenges; Incident Response
- Suppliers/partners
Challenges in creation of ISAC’s

- Finding technical expertise in cybersecurity
- Not enough resources & funding (Expertise, tools, management)
- Non binding, collaboration mode
- Conflicts of interests
- Trust amongst members/partners
ER - ISAC

Administrative management: Information Sharing

One voice in Europe for the cybersecurity in the Railway

ER-ISAC
ER - ISAC

Administrative management: Analysis Center

One playground in Europe for the cybersecurity in the Railway

- GSM-R Anti jamming
- NIS Directive cross border security measures
- Control Center systems resilience
- Railway cyber threats landscape
- Railway Minimum Cybersecurity measures
- Cybersecurity in ERTMS
- Cybersecurity in EU Railway (stream Unife/DG Move)
- Other ISAC’s
- WG Architecture

Working Group running
Kick off done or planned
Kick off to start
How is the Cybersecurity for the Railway in Europe is sharing cybersecurity threats between organisations and Countries

Speaker: Olivier De Visscher, Cyber Security Adviser Infrabel, Co-Chair of the European Rail Information Sharing and Analysis Center (ER-ISAC), Belgium
Information Sharing and Analysis Center (ISAC)

Non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow “two-way” sharing of information between the private and the public sector.

ISACs have created communities within the private sector.

They could be oriented on a specific critical sector (e.g. transport) to gather information about cyber incidents and analyze it.
ER - ISAC

ER ISAC (establishing data-sharing protocol and one organization for railway in EU)

- Members of ISACs exchange information about threats, incidents, vulnerabilities, mitigating measures and also about the best practices and tools.

- The most common tool for exchanging information is a special web portal/platform (following a specific template) and encrypted emails.

- Among the ISACs, there is a common practice to establish so called “circles of trust”.

- Most ISACs use the Traffic Light Protocol (TLP) to share information. It is not necessary to share Red or Yellow TLP categorized information to allow sharing cybersecurity threats.

- Some ISACs also receive information from external sources (e.g. IT security companies) what is very good practice.