



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

Workshop on cybersecurity in Inland Navigation

Introduction to Railway Systems

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

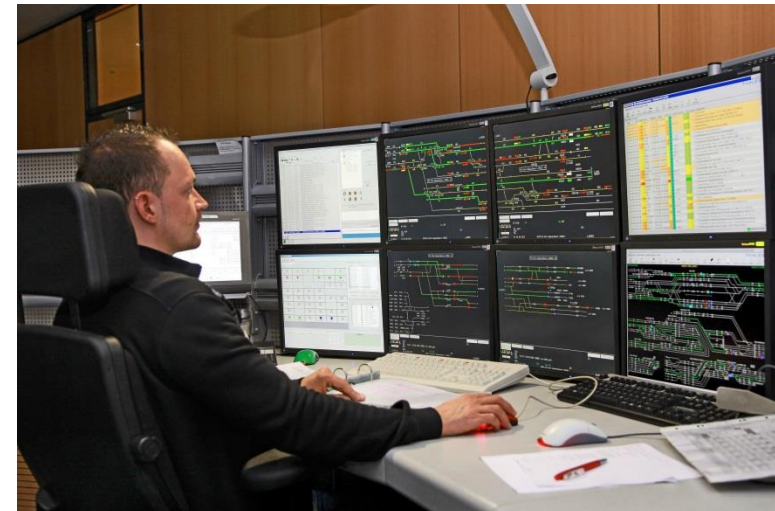
- Stations as gate to railway transportation
- Europe-wide rail networks

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

- 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



Home	Monitor-Konfiguration	Netzwerk-Konfiguration
	<ul style="list-style-type: none"> • Büro 0 • Email 	
<hr/> transtec transtec Hotline		
	<ul style="list-style-type: none"> • Netzwerk-Probleme während der Installation • Büro 069-265-37200 	
<hr/> Benutzerkonten Passwörter		

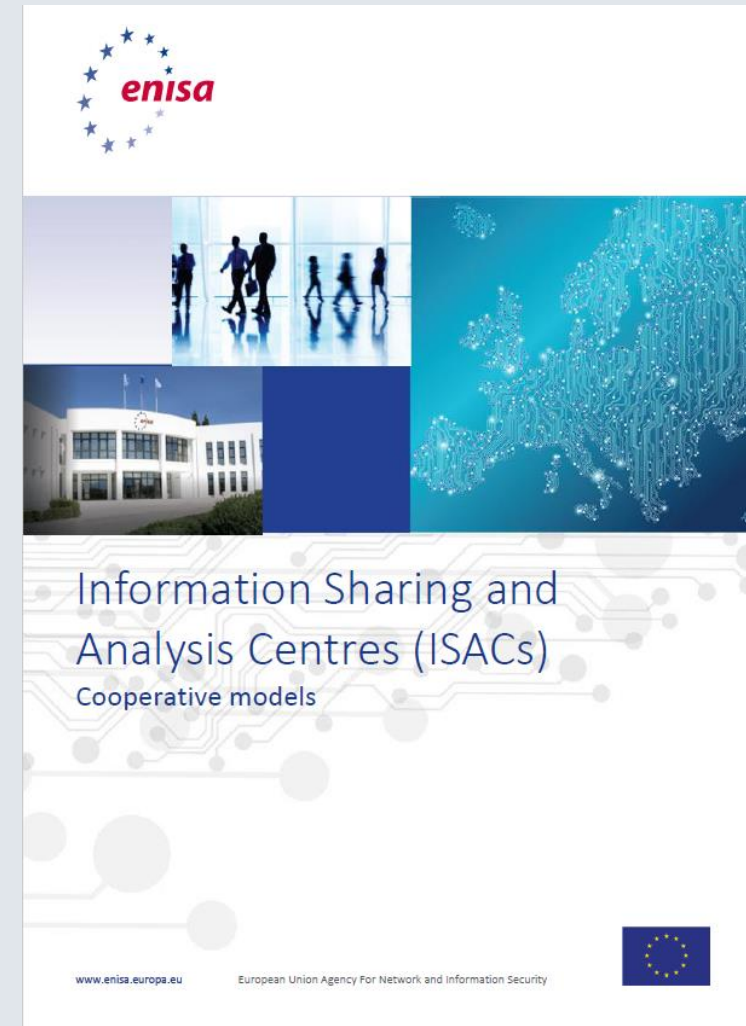
- **Netzwerk-Probleme** während der Installation
- Büro 069-265-37200

Benutzerkonten **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

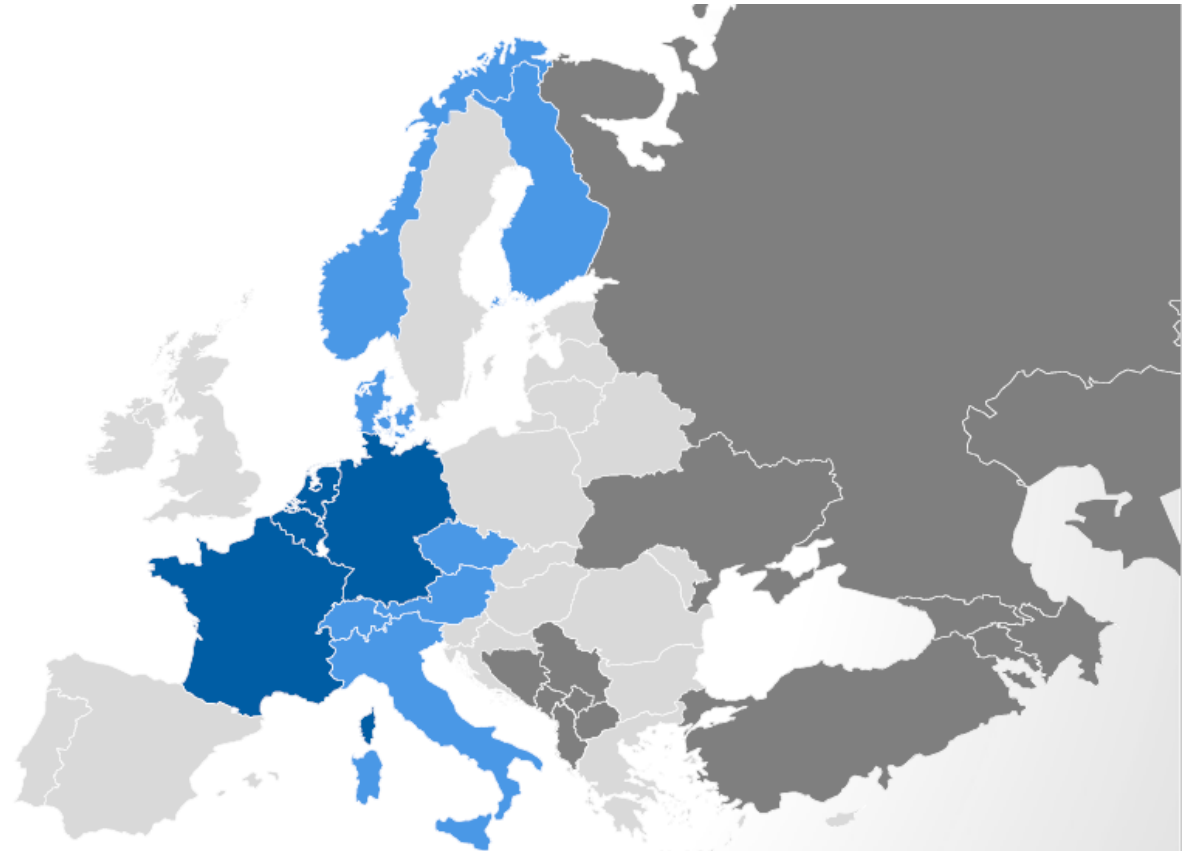
FI / NO / DK / IT / CH / AT / CZ



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

- 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

4	1	Scope	6
5	2	Normative references	7
6	2.1	Future Developments of IEC 62443 Series	7
7	3	Terms, definitions and abbreviations	8
8	3.1	Reference:	8
9	3.2	Terms	8
10	3.3	Abbreviations	20
11	3.4	Verbal forms	21
12	4	Cybersecurity within a Railway System Life Cycle	22
13	4.1	Railway system and product life cycles	22
14	4.2	Activities, synchronization and deliverables	22
15	4.3	Relationship between cybersecurity and safety	28
16	4.4	Assurance process	30
17	5	System Specification	32
18	5.1	Railway System	32
19	5.2	Railway Asset Reference Model	33
20	5.3	Railway Physical Architecture Model	34
21	5.4	Railway Zoning and Segmentation Model	34
22	5.5	The Rail Reference Architecture	37
23	6	System Definition and High-Level Risk Assessment	40
24	6.1	Introduction	40
25	6.2	SuC - System under consideration	40
26	6.3	Essential functions	41
27	6.4	Assets supporting the essential functions	42
28	6.5	Threat landscape	42
29	6.6	High level risk assessment process	42
30	6.7	Zones and conduits of the SuC	44
31	7	Detailed Risk Assessment	46
32	7.1	General aspects	46
33	7.2	Establishment of Security Requirements	47
34	8	Security requirements	58
35	8.1	Objectives	58
36	8.2	Foundational Security Requirements	58
37	8.3	Apportionment of Security Requirements	75
38	9	System Assurance and Acceptance for Operation	78
39	9.1	Overview	78
40	9.2	Cybersecurity Case	78
41	9.3	System Security Integration Assurance	79
42	9.4	System Security Assurance (Validation)	82
43	9.5	System Acceptance	83
44	10	Operational, maintenance and disposal requirements	84
45	10.1	Introduction	84
46	10.2	Identify, Protect, Detect, Respond, Recover	84
47	10.3	Security Supply Chain Management / Supplier Management	85
48	10.4	Maintenance	86
49	10.5	Network and communication security	86

50	10.6	Patch management	87
51	10.7	Operational Requirements	88
52	10.8	Event and incident management	89
53	Annex A (informative)	Handling conduits	91
54	A.1	Introduction	91
55	A.2	Requirements for conduits in IEC 62443	91
56	A.3	Protection Profiles for Conduits	92
57	Annex B (informative)	Handling Legacy Systems	93
58	B.1	Introduction	93
59	B.2	Basic Security risks	93
60	B.3	Basic Process Activities	94
61	B.4	Basic Security Countermeasures	96
62	Annex C (informative)	Security Design Principle	99
63	C.1	Introduction	99
64	C.2	Secure the weakest link	100
65	C.3	Defence-in-depth	102
66	C.4	Fail secure	104
67	C.5	Grant least privilege	106
68	C.6	Economise mechanism	108
69	C.7	Authenticate requests	111
70	C.8	Control Access	113
71	C.9	Assume secrets not safe	115
72	C.10	Make security usable	117
73	C.11	Promote privacy	119
74	C.12	Audit and monitor	121
75	C.13	Proportionality principle	123
76	C.14	Precautionary principle	124
77	C.15	Continuous Protection	126
78	C.16	Secure Metadata	127
79	C.17	Secure Defaults	128
80	C.18	Trusted Components	130
81	Annex D (informative)	Safety and Security	131
82	D.1	Introduction	131
83	D.2	The differences between safety and security	131
84	D.3	Security from a safety perspective	132
85	D.4	Co-Engineering of Safety and Security	132
86	D.5	Quantification of Security	133
87	D.6	The relationship of Safety Integrity Levels and Security Levels	133
88	D.7	Responsibility for Security	134
89	Annex E (informative)	Risk Acceptance Methods	135
90	E.1	Introduction	135
91	E.2	Example based on EN 50126	135
92	E.3	Example Method (System Integrator)	138
93	E.4	Example method (Operator)	140
94	Annex F (normative)	Generic Security Requirements and Cross-reference Table ..	143
95	F.1	Generic Security Requirements (Normative)	143
96	F.2	Security Requirements Cross-reference Table (Informative)	163

How can the Inland Navigation benefit from cooperation

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

<http://www.er-isac.eu>

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