



# 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**

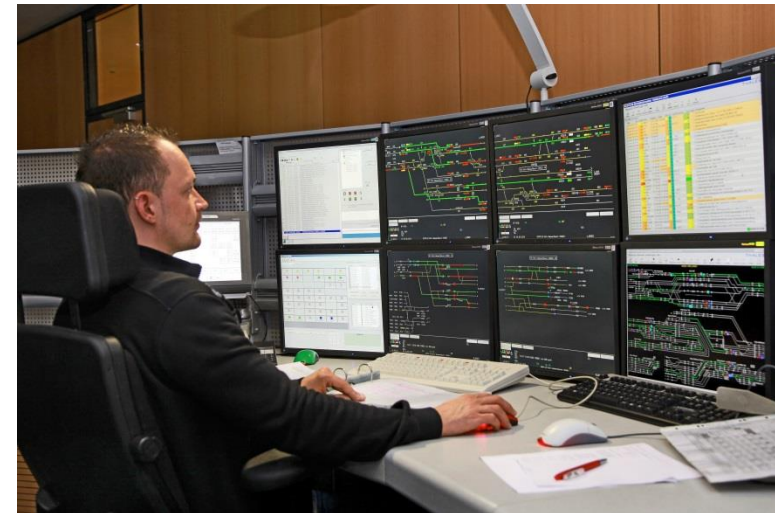
- Stations as gate to railway transportation
- Europe-wide rail networks

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

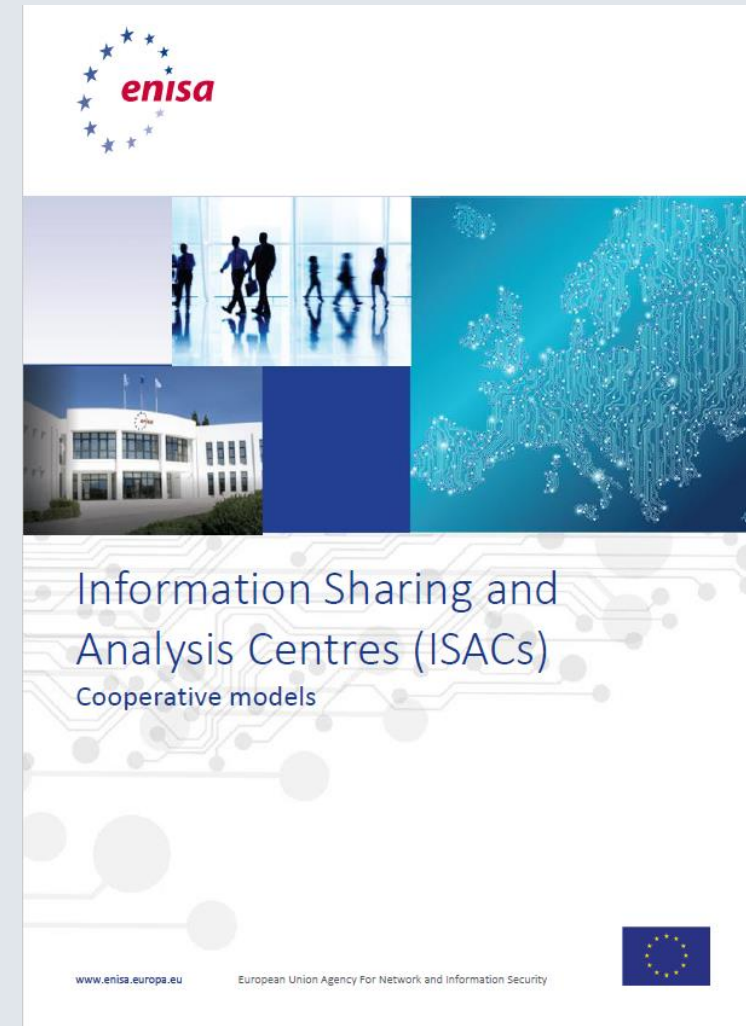
- **Netzwerk-Probleme** während der Installation
- Büro 069-265-37200

### **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

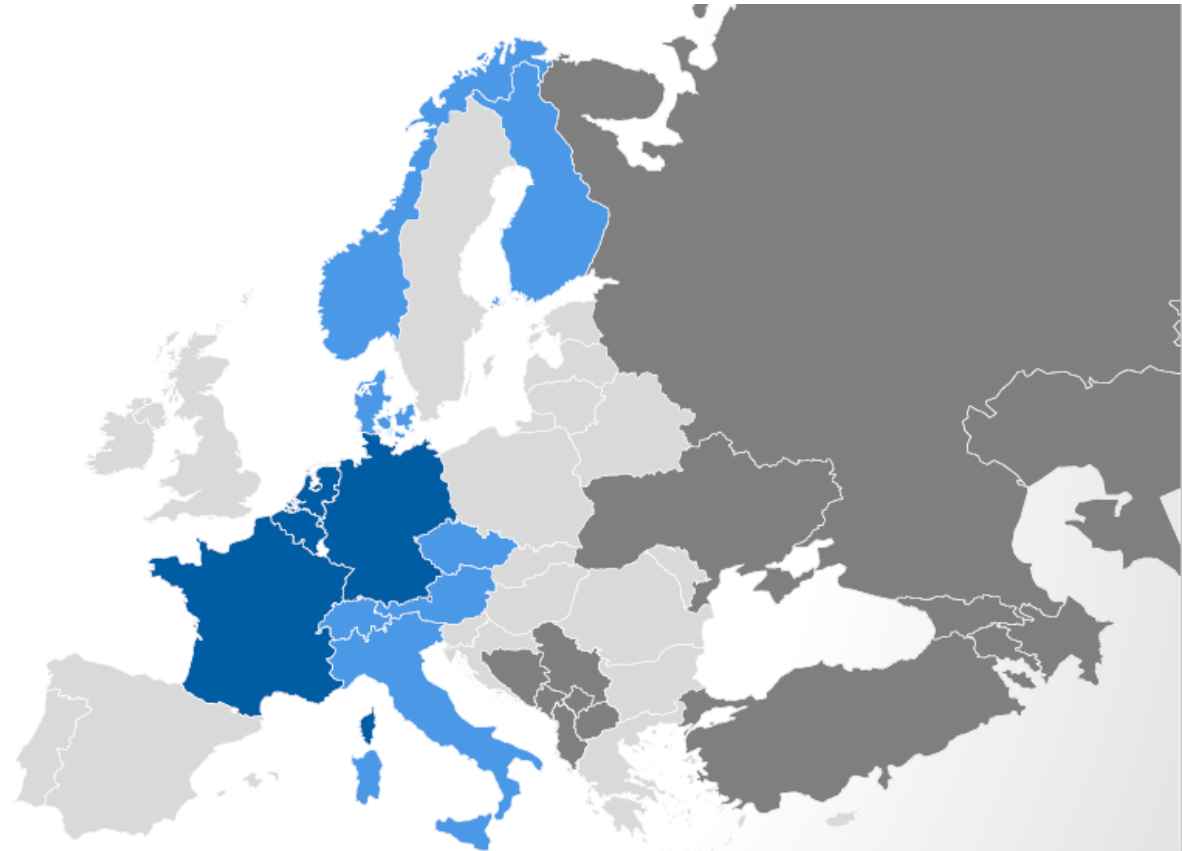
FI / NO / DK / IT / CH / AT / CZ



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

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

# 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](mailto:christian.schlehuber@deutschebahn.com)

[contact@er-isac.eu](mailto:contact@er-isac.eu)

[www.er-isac.eu](http://www.er-isac.eu)