ENISA MARITIME CYBERSECURITY WORKSHOP

Lisbon 26th of November 2019

European Rail Information Sharing and Analysis Center (ER-ISAC)

Good practices from European Rail ISAC

Presented by
Olivier de Visscher
ER-ISAC Chairman

Reach us at : Contact@ER-ISAC.EU

Best practices from the ER-ISAC

3 stages of an ISAC

- Before the creation of the ISAC
- While running the ISAC
- Once the ISAC is fully operational

Before the creation of the ISAC

- **Raise interest to the widest audience possible**

Through your European Agency, the supporting organisations, the lobbies, the EU Cybersecurity agency, your industry Information Security peers for discussions meetings

- ➢ Raise interest / Understand challenges (Regulatory, Standardisation, Operations)
- ➢ Allow assessing areas of collaboration
- ➢ Willingness
- ➢ Broader communication (through the members of those organisations/lobbies)
- ➢ Create Working Groups by interest groups to avoid conflicts

- **Avoid perfection**

Do not target a perfect organisation by thinking of All cases/issues

- ➢ Terms of Reference as light as possible,
- ➢ Start thinking of TLP White & Green information that could be shared to get trust in collaborating
- ➢ Give CEO & Legal offices confidence
- ➢ Focus on making the collaboration affordable to most of organisation

ER - ISAC

While running the ISAC

- **Identify your similarities / the basis for collaboration**

➢ Start by sharing, to a large amount of members, your setup, infrastructure, critical processes, supporting assets, supporting supply chain & agree on a common IT/OT Landscape *(position paper)*

➢ Share views and knowledge on Threats to your sector (*Opinion paper*)

- **Assess the on-going Cybersecurity Initiatives**

➢ GAP analysis on IT/OT common landscape

➢ Identify areas for collaboration

- **Use assistance of new EU ISAC Facilitator**

➢ Secure platform, ISAC administration, Governance, …

- **Get expertise**

➢ Find common areas of expertise through Inter ISAC (SCADA's – Energy, Cloud/IoT – Finance,Safety related systems – Aviation/Rail, Communication – Telecom)

ER - ISAC

Once the ISAC is fully operational

- **Support & Sustainability**

➢ Support services & Administration through membership

- **Advertise the key success & deliverables**

➢ Provide to your stakeholders (CEO’s) concrete contributions

- **Identify and describe processes and services**

➢ Services expected from the ISAC (Trainings, Cross border exercises, Threat intelligence, …)

- **Develop Vulnerability management**

➢ Share Indicator of Compromise (depending of Members maturity)

Quick facts on ER-ISAC

- Acting in Standardisation : Cenelec WG 26 dedicated to Cybersecurity for Railway Systems
- Acting in Cybersecurity by default : Threat Landscape vs Minimum CyberSecurity Baseline for Railway systems
- Acting on International : United Nations (Europe / Asia Rail Transport Corridors Cybersecurity)
- Acting on Architecture : Working Group dedicated to OT landscape
- Acting Cross sector : Collaboration potential areas identified with Telecom, Energy and Aviation

ER - ISAC

Members per Countries (Sept 2019)

Nearly 54 organisations since foundation on 4th of June 2019

Co Chair

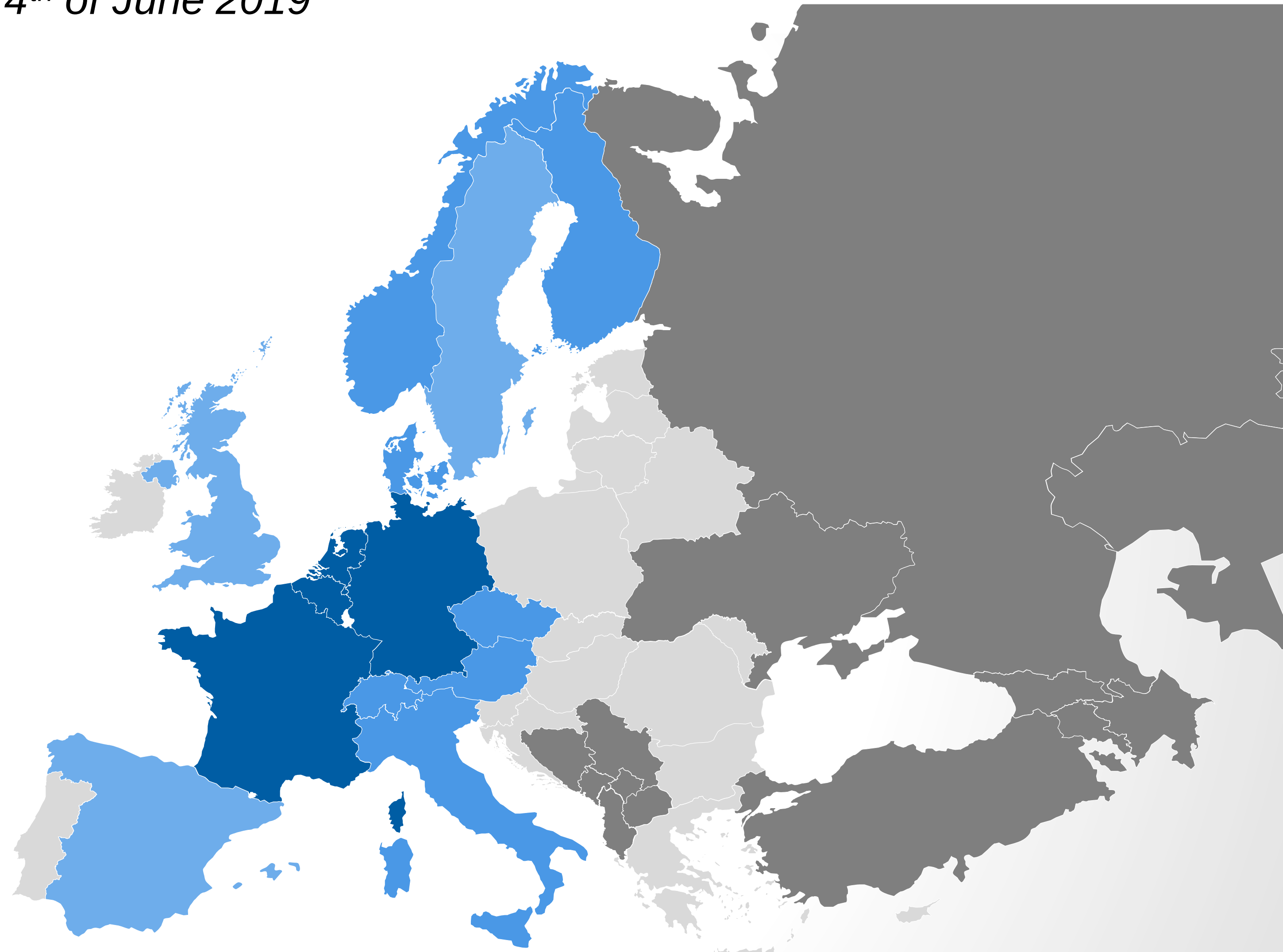
FR /DE /BE /NL

Members

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

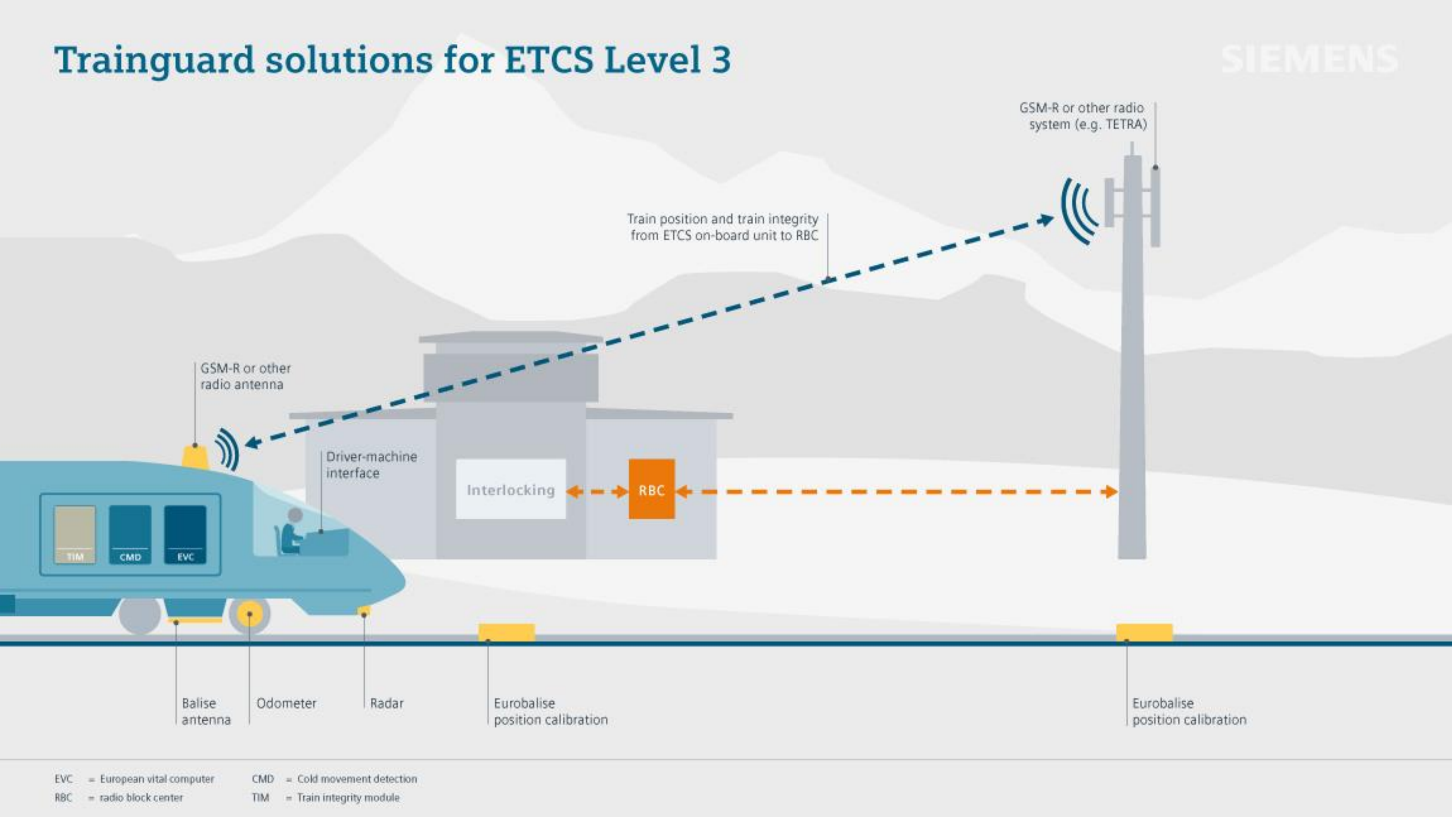
Members to be contacted

Possible future partnership



ER - ISAC

Why collaborate in cybersecurity in the Railway ?


Trainguard solutions for ETCS Level 3
SIEMENS
GSM-R or other radio system (e.g. TETRA)
Train position and train integrity from ETCS on-board unit to RBC
GSM-R or other radio antenna
Driver-machine interface
Interlocking
RBC
TIM
CMD
EVC
Balise antenna
Odometer
Radar
Eurobalise position calibration
Eurobalise position calibration
EVC = European vital computer
RBC = radio block center
CMD = Cold movement detection
TIM = Train integrity module

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

Specific technologies for Signalling systems

Same supply chain

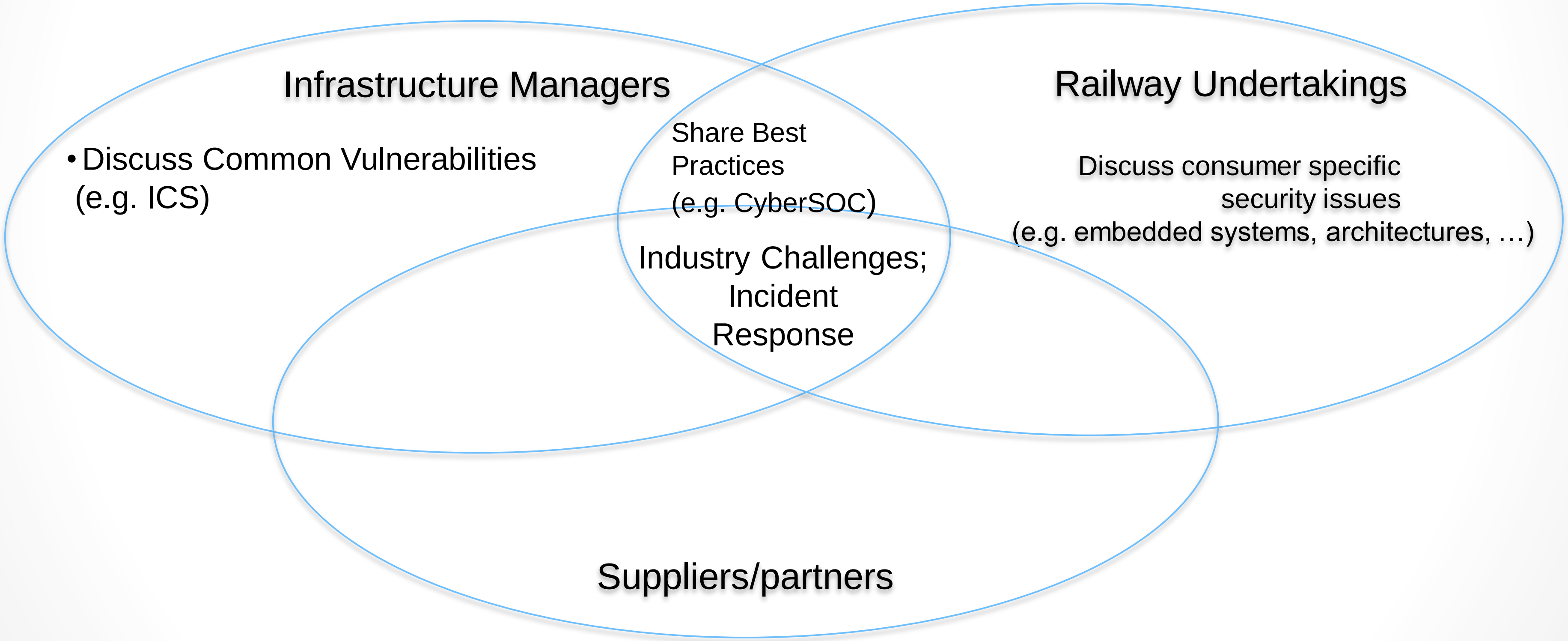
Specific Standardisation for Safety in the Railway

=> One issue affects us All

” into the Railway Undertakings bubble

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



Infrastructure Managers

- Discuss Common Vulnerabilities (e.g. ICS)

Share Best Practices
(e.g. CyberSOC)

Industry Challenges;
Incident
Response

Railway Undertakings

Discuss consumer specific
security issues
(e.g. embedded systems, architectures, …)

Suppliers/partners