ER - ISAC

UNECE

OSCE Organization for Security and Co-operation in Europe

# Session II – The role of government authorities in facilitating technology driven solutions to improve security of inland freight routes

- **Development of cyber threat mitigation measures at national and international levels**

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

DB DB NETZE INFRABEL Right On Track B SNCF RÉSEAU SNCF MOBILITÉS ProRail

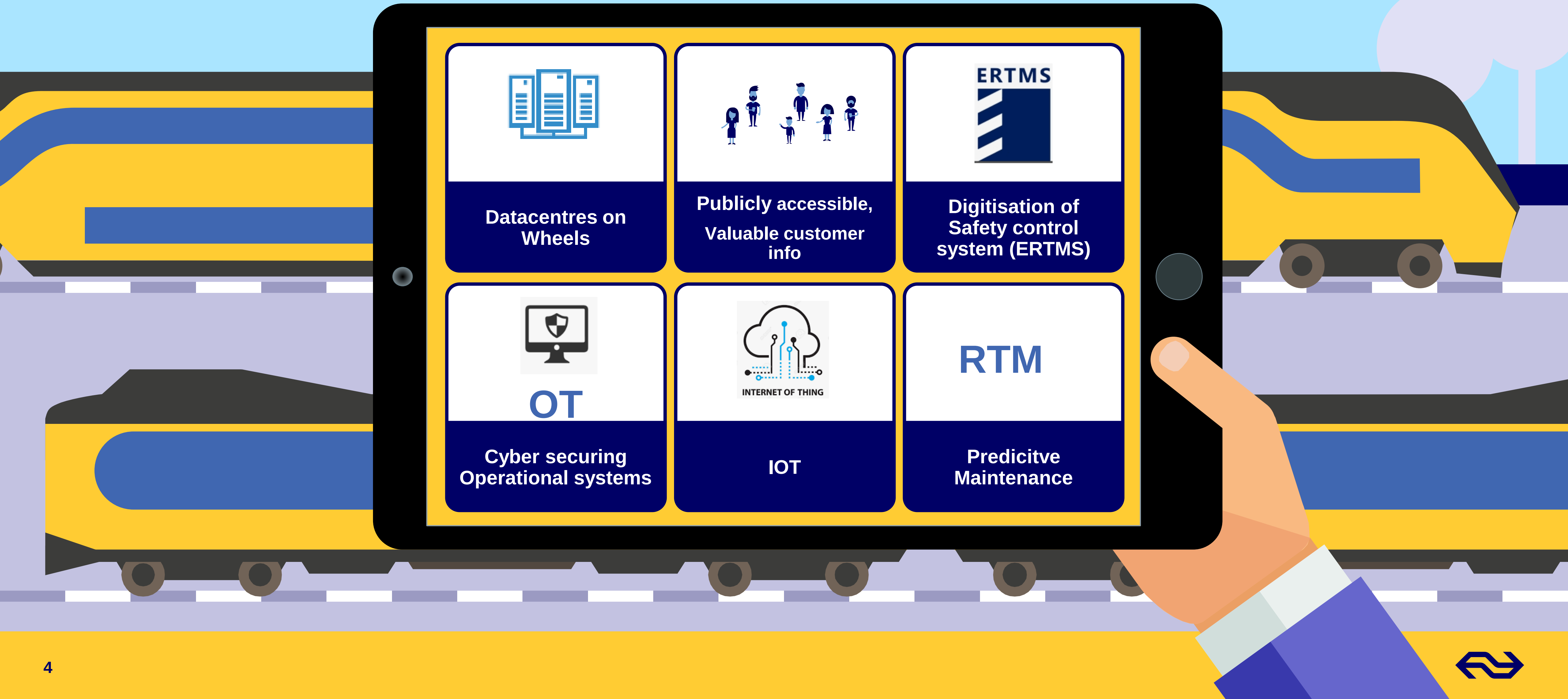
# European Rail Information Sharing and Analysis Center (ER-ISAC)

Presented by Olivier de Visscher
On behalf of
ER-ISAC Co Chair

# 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 chalenges

# Digitisation of Trains introduces cyber risks



Datacentres on Wheels

Publicly accessible,

Valuable customer info

ERTMS

Digitisation of Safety control system (ERTMS)

OT

Cyber securing Operational systems

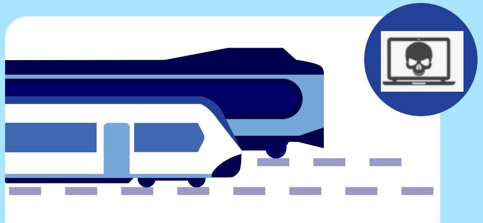
IOT

RTM

Predicitve Maintenance

# There is a great need for policy and oversight

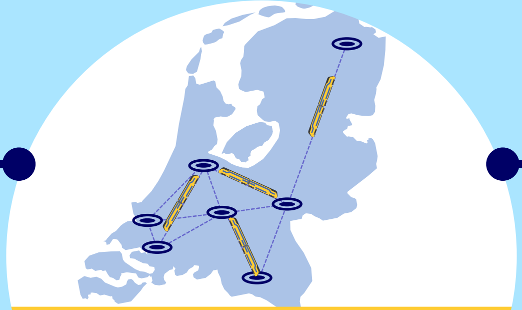
Rail Industry
cyber risk control is
immature



Threats sophistication
increases threat surface

=

increase incidents



Critical Infrastrucure?
Regulation
Standardisation

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 2018

WannaCry attacks,

Deutsche Bahn, ticketing
and information systems

Germany's rail network

May 2017

Actually happened

Four cyber attacks on Uk
Railways

July 2016

Chaos Computer Club, 32nd
congres, Hamburg,
December 27, 2015

NON DISCLOSED

Hypothetically
possible

# ER - ISAC

## 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.

Source : ENISA - *https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models*

# ER - ISAC

## Members per Countries (Sept 2019)

*Nearly 50 organisations since foundation on 4th of June 2019*

### Co Chair

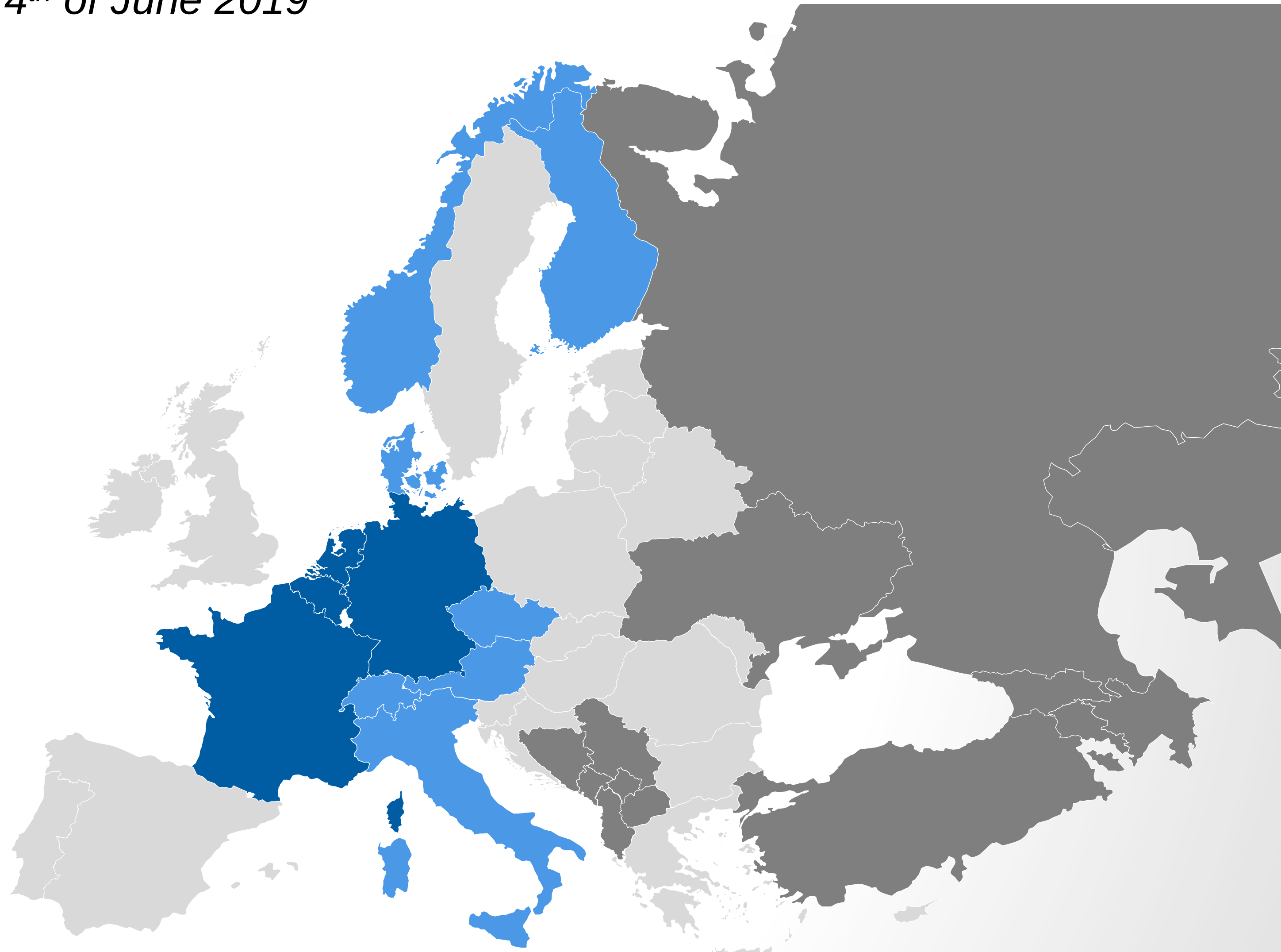
**FR /DE /BE /NL**

### Members

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

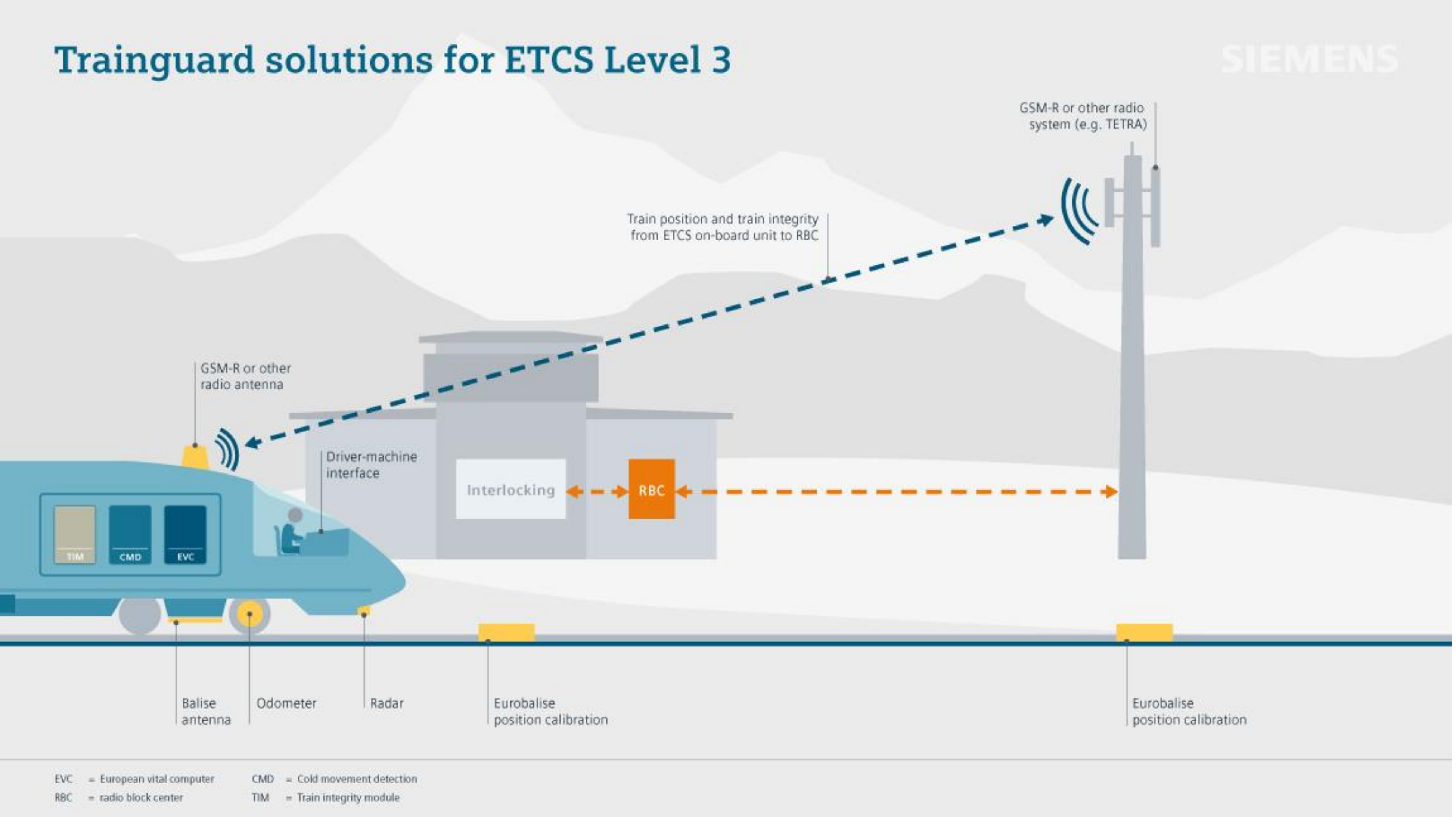
### Members to be contacted

### 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

UNECE

OSCE Organization for Security and Co-operation in Europe

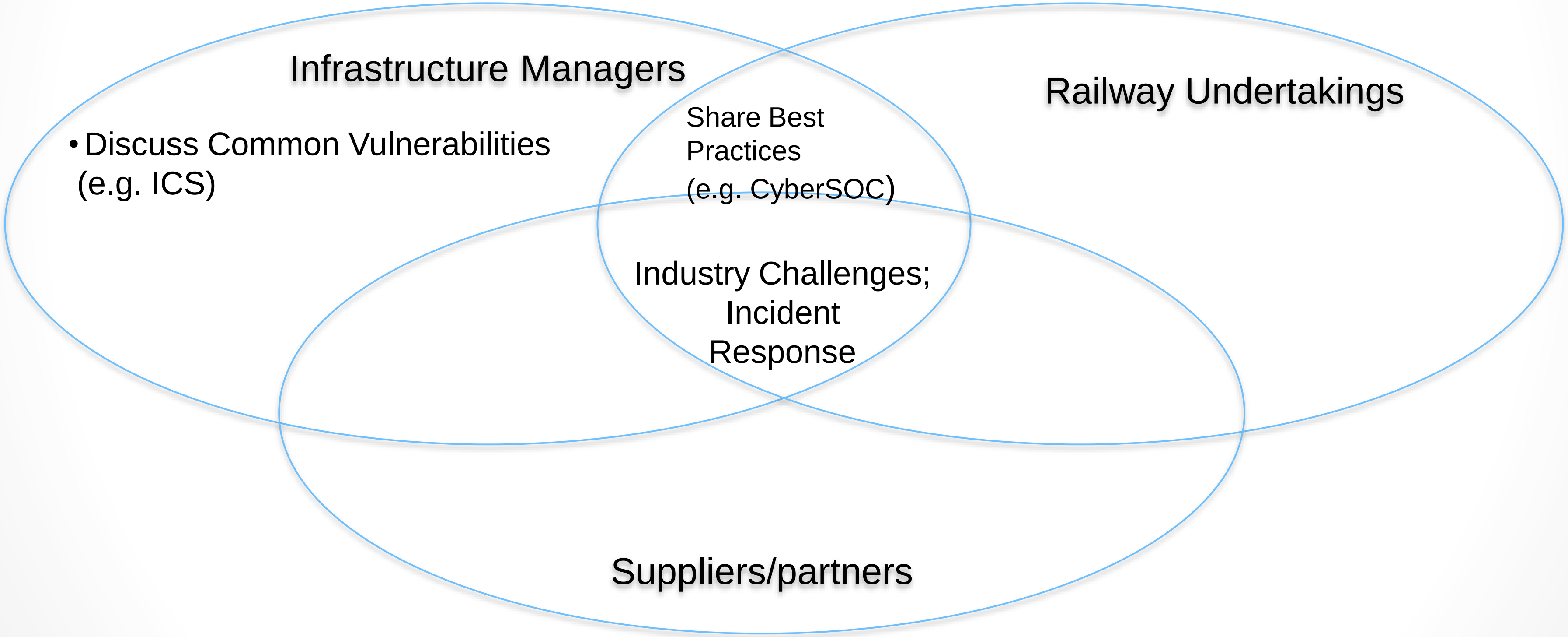
# How will the EU Railway Cybersecurity Platform (ISAC) help us

## 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



Infrastructure Managers

- Discuss Common Vulnerabilities (e.g. ICS)

Share Best Practices

(e.g. CyberSOC)

Railway Undertakings

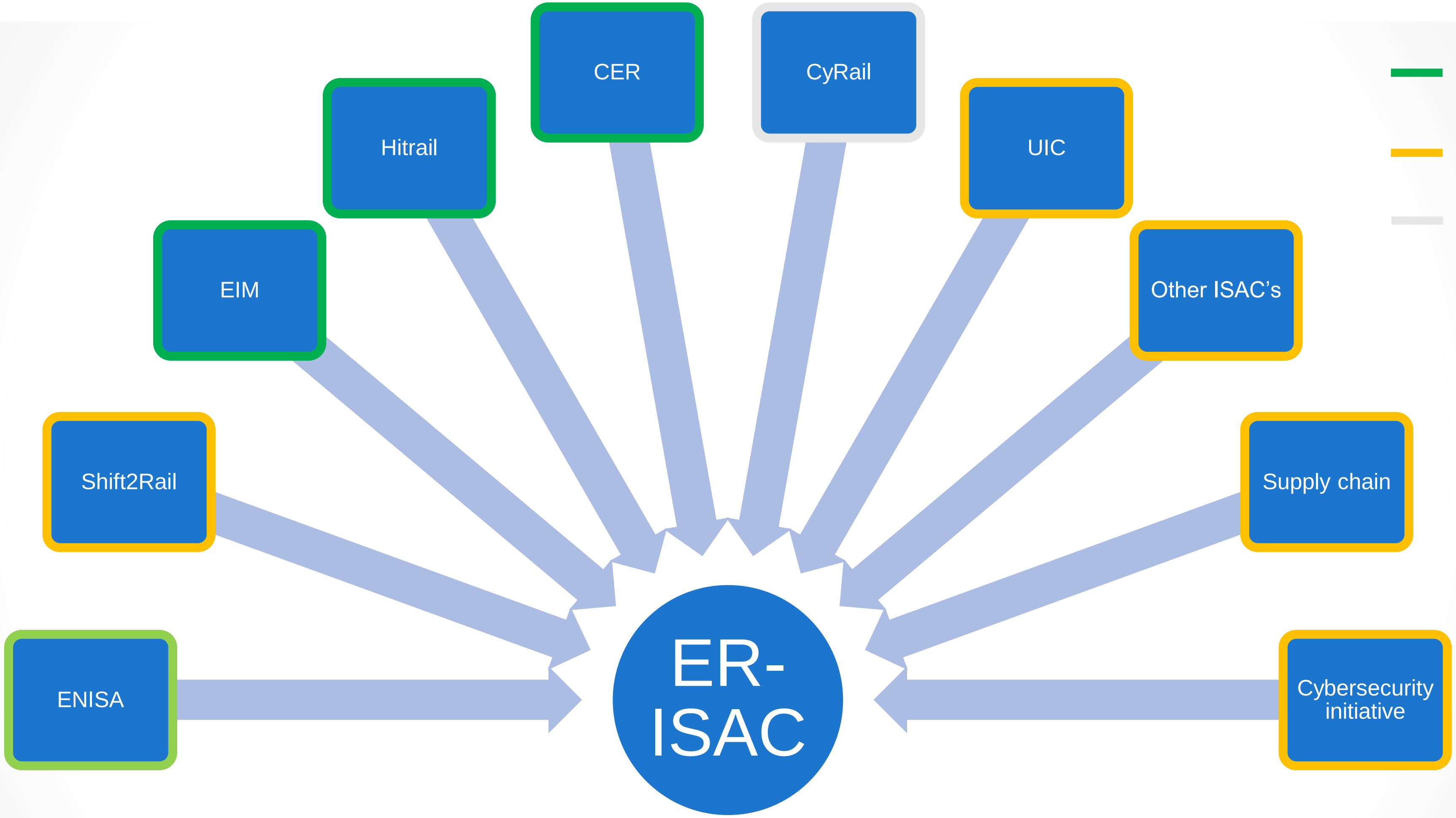
Industry Challenges; Incident Response

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

# Administrative management: Information Sharing



CER

CyRail

Hitrail

UIC

EIM

Other ISAC’s

Shift2Rail

Supply chain

ENISA

ER-ISAC

Cybersecurity initiative

🟩 Already connected /presented their contribution

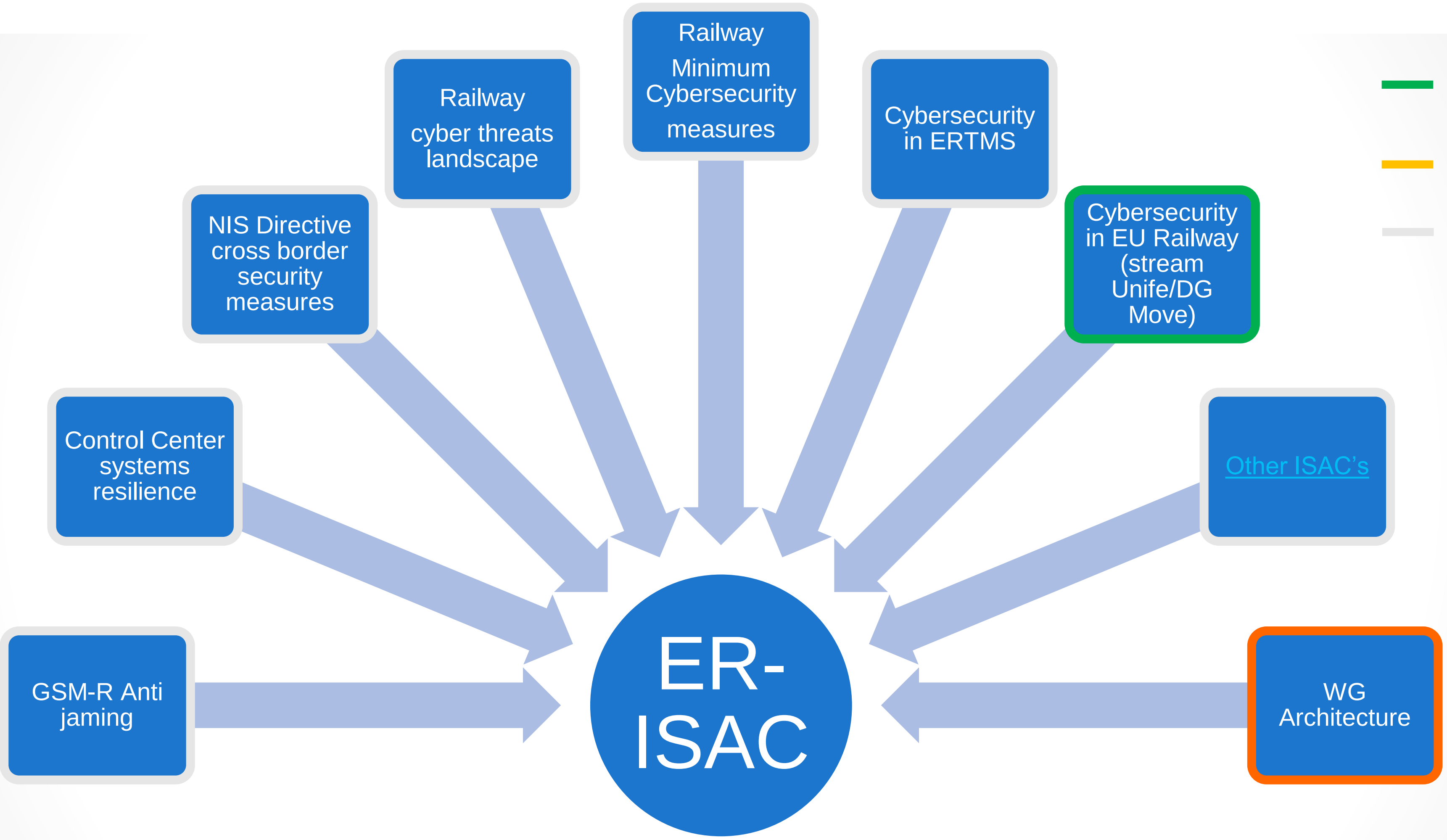
🟨 To be contacted / presentation next plenary in Dec.

⬜ Will be coming soon

One voice in Europe for the cybersecurity in the Railway

# ER - ISAC

## Administrative management: Analysis Center


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

🟩 Working Group running

🟨 Kick off done or planned

⬜ Kick off to start

One playground in Europe for the cybersecurity in the Railway

# Session III – The way forward – How to move from theory to practice?

- Establishing structured mechanisms for the exchange of information on threats and risks along supply chains (i.e. transport corridor based), involving multiple stakeholders such as law enforcement, customs and border management agencies but also transport authorities and private sector operators.

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

# ER - ISAC

UNECE

OSCE Organization for Security and Co-operation in Europe

## The strength of Unity

- Creation of Experts from suppliers, industry, specific 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**)
- Integrate certification bodies to adapt standards to cybersecurity context (**Cybersecurity by default**)
- Integrate R&D innovation project as a governance body / testing body (**Continuous protection**)
- Assess and create minimum security baseline to enforce it into supply chain (**Cybersecurity by design**)
- Involve Locals Governments CSIRT’s to assist in cross borders risks (**Cyber resilience**)