











Olivier.devisscher@er-isac.eu





## What is it?

The ER-ISAC is a non-profit organization that provides a central resource for gathering information on cyber threats as well as allowing a two-way sharing of information between the private and the public sector about root causes, incidents and threats, as well as sharing experience, knowledge and analysis.(\*)

It is sponsored by UIC that helps providing the sustainability of the collectivity through membership.

The community is composed of experts from the Cybersecurity and Rail Industry.

The scope is focused on securing the technologies that supports our Railway through Cybersecurity practices.

## **Main Activities**

Through dedicated Working Groups / selected Groups of discussions, it is possible to collaborate without risks of competitions or collateral damage (Public procurement rules, Regulatory issues, Cybersecurity threats)

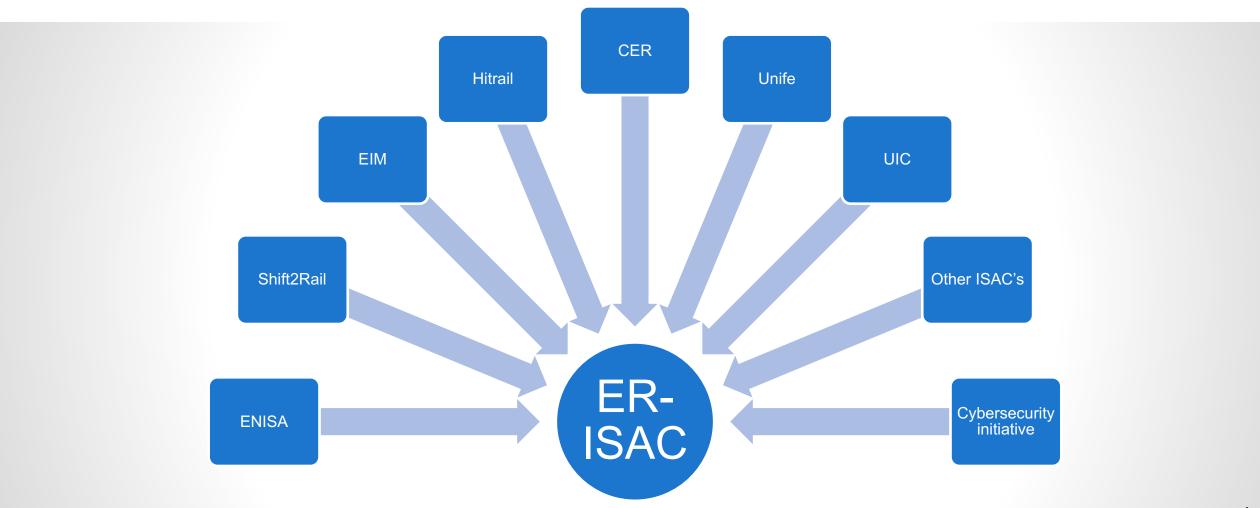
#### **Information Sharing:**

Sharing information gathered from cross borders operational projects, Cybersecurity initiatives, Threats and vulnerabilities, Awareness and contribution (Promoting the work of ER-ISAC, collaborating with others ISAC's, contributing to international communities / Cybersecurity Rail conferences)

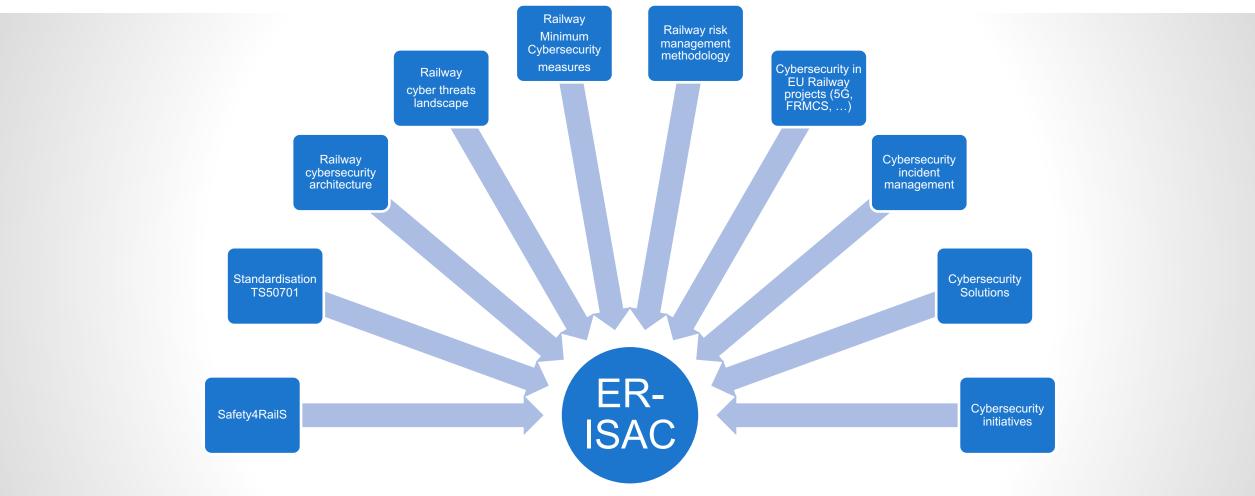
#### **Analysis Center:**

Providing and producing cybersecurity analysis, major topics addressed through specific WG (Cybersecurity Architecture, Minimum Cybersecurity Measures, Threat Landscape, NIS Directive, ...), links with others ISAC's (Energy, Aviation, Finance, Maritime, Telecom, ...) and agencies/bodies (ERA, ENISA, DG-Move, DG-Connect, ...)

# **Information Sharing**



## **Analysis Center**



One playground in Europe for the cybersecurity in the Railway

# Key principles of organisation

#### Roles:

- Chairman / Facilitator : General coordination and logistics, reporting, communication of ER-ISAC initiatives, promoting, connection with other organisations, ...
- Co-Chair : General gouvernance
- Members : IMs and RUs from Europe
- Partners: Suppliers (Commercial organisations active in the rail sector), European or national bodies (Public Authorities, ER-ISAC or EU financed bodies), Research centres (universities, ..), Other ISACs

ER-ISAC hosted/sponsored by UIC as UIC-Project (start in Q2/2020) - Guarantee of independence

Funded by members and partners-suppliers

Two General Assemblies by year (with for each, one members-only session & one opened-session)

See « Term Of Reference » for more details

# **Members per Countries (March 2021)**

49 organisations since foundation on 4<sup>th</sup> of June 2019



Co-Chair FR /DE /BE /NL



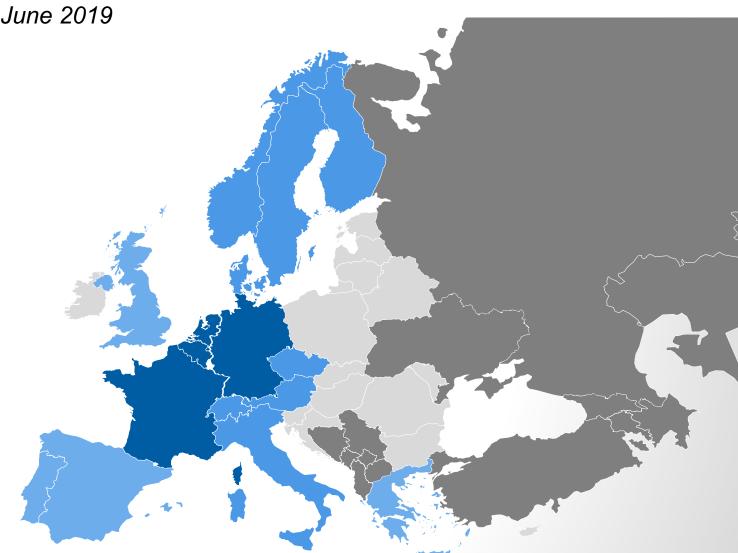
**Members** 

/NO /DK /IT /CH /AT /CZ /LU /ES /PT /GR /SE

Members to be contacted



Possible future partnership



## **Annexes**

## **Services / initiatives Roadmap**



Self financing the ER-ISAC



Providing the Community with a set of secured platforms to communicate, share and produce information



Sharing information gathered from cross borders operational projects, Cybersecurity initatives, Threats and vulneabilities



Providing and producing cybersecurity analysis



Promoting the work of ER-ISAC, collaborating with others ISAC's, contributing to international communities / Cybersecurity Rail conferences

ER-ISAC self financing

ER-ISAC IT Secure platforms

ER-ISAC Information sharing

ER-ISAC Analysis Center **ER-ISAC** 

Awareness and contributions

## Services / initiatives Roadmap \*

- (I) Status and Terms of Reference
   (I) Membership
- (I) Cyber/information security incident platform
- (I) Information sharing
- (I) Vulnerability management
- (I) ER-ISAC Dashboard
- (I) Internet & Intranet page

- (S) Threats and risks (facilitator

   intel isacs and others sources)
- (S) Cybersecurity initiatives / major operational projects (UIC, ERA, DG Move,...)
- (S) Intra ISAC Info sharing
- (S) Initiatives reporting
   (facilitator centralisation)
- (S) Trainings & Awareness:
   ENISA support workshops, members cases,
- (S) Cybercrisis exercises and guidelines
- (S) ER-ISAC publications (reports, opinion and position papers, ...)

- (I) Threat landscape (facilitator)
- (I) Digitalising WG Unife/DG Move: GAP Analysis, recommendations on Rail Cybersecurity (Unife)
- (I) Cybersecurity
   architecture: mapping Critical
  functions/Assets/supply chain (NS)
- (I) Standardisation: TS 50701
- (I) NIS Directive sec

measures: Study Min.sec.baseline (Enisa)

- (I) Min.Security baseline (facilitator)
- (I) CyberSoc

implementations review (S2R)

- (I) Risk management methodologies (S2R)
- (I) ERTMS cybersecurity (ERA/UNISIG)
- (I) Safety4RailS (UIC)

- (S) Railway events contribution
- (S) ER-ISAC events
- (S) ER-ISAC advisory
- (S) Others sectors contribution

ER-ISAC self financing

ER-ISAC
IT Secured platforms

ER-ISAC Information sharing

ER-ISAC Analysis Center ER-ISAC
Awareness and contributions

Legend	
(S)	Services
(I)	Initiatives

<sup>\*</sup> Subject to availability of resources