# The European rail supply industry's position on cybersecurity in railway transport

**ERA&ENISA conference**

**Nicolas Furio – UNIFE Head of Technical Affairs**

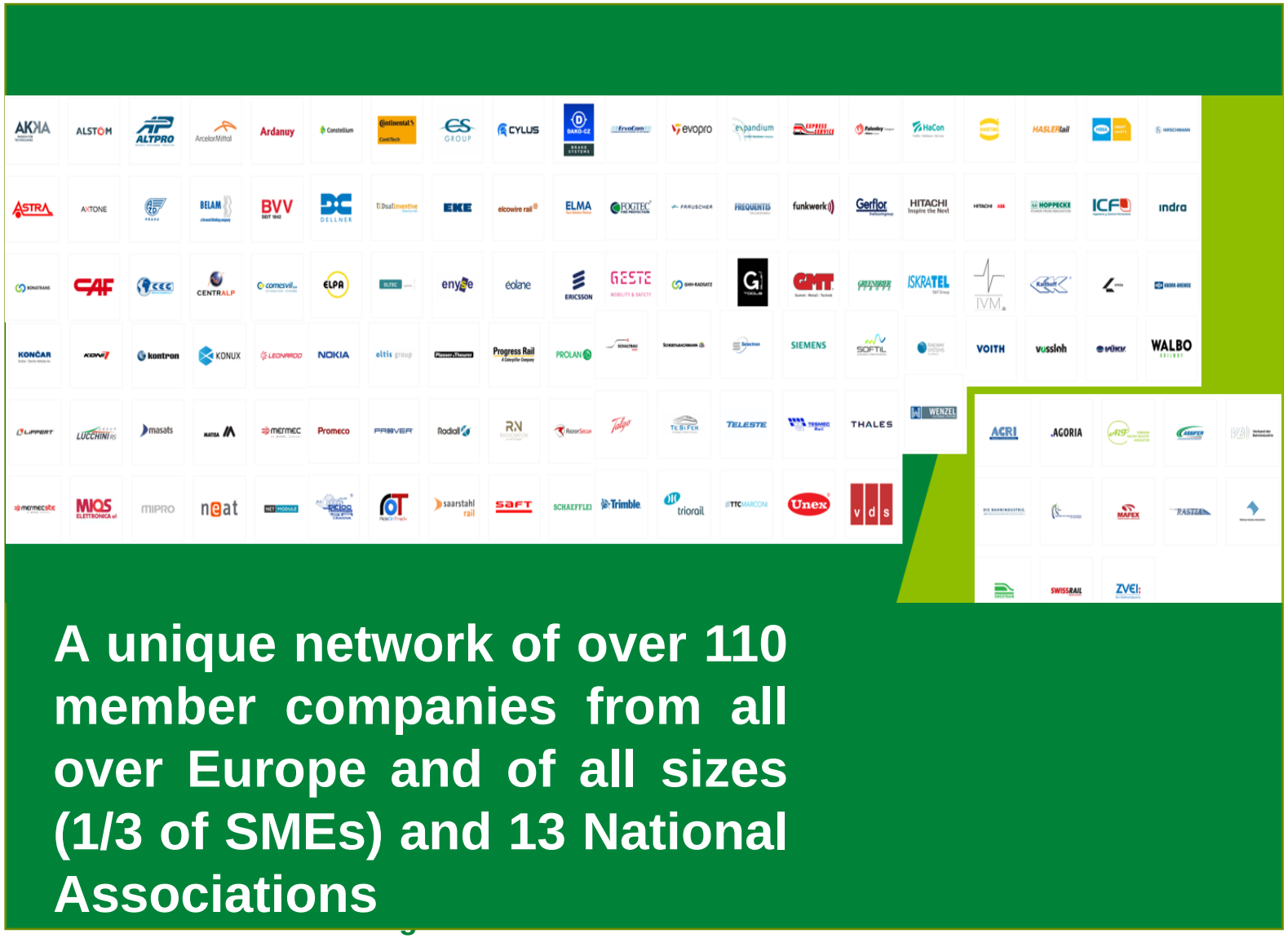
**Lille, 1st December**

# UNIFE – The European Rail Supply Industry Association

**UNIFE** represents the European Rail Supply Industry in Brussels since 1992.

- The association gathers **more than 110 of Europe's leading large and medium-sized rail supply companies** active in the design, manufacture, maintenance, and refurbishment of rail transport systems, subsystems and related equipment.

- UNIFE also brings together 13 national rail industry associations of European countries. For more information, visit www.unife.org or follow @unife on Twitter and LinkedIn.




unife
THE EUROPEAN RAIL INDUSTRY

# UNIFE – Why is cybersecurity so important?

## Importance of cybersecurity in railways

**UNIFE** considers cybersecurity as one of the key priorities in the rail sector. Cybersecurity is key for the digital transformation of the European rail sector.

- ✓ **Digitalisation** is at the heart of the development of railway transport in order to increase notably capacity, reliability and performance. Rail companies have already implemented a vast array of new services and applications using digital technologies.

- ✓ **Current threat landscape is evolving fast:** the volume and complexity of cyber attacks is increasing quickly.

- ✓ **Legislative framework:** Cybersecurity is becoming important and more regulated. The new regulation framework aims notably at harmonising responses when addressing cybersecurity.

# UNIFE – Why is cybersecurity so important?

## Collaboration: Key enabler to success in cybersecurity in railways

**Collaboration** within the rail sector is key to face the challenges linked with the increase of cyber threats and attacks.

The implementation of a fully cyber resilient railway transport rely on:

- The capacity of the rail sector to **build trust** between its stakeholders
- **Avoiding silos** at every level of cybersecurity detection, analysis and response

## Commitment of the European Rail Supply Industry regarding cybersecurity

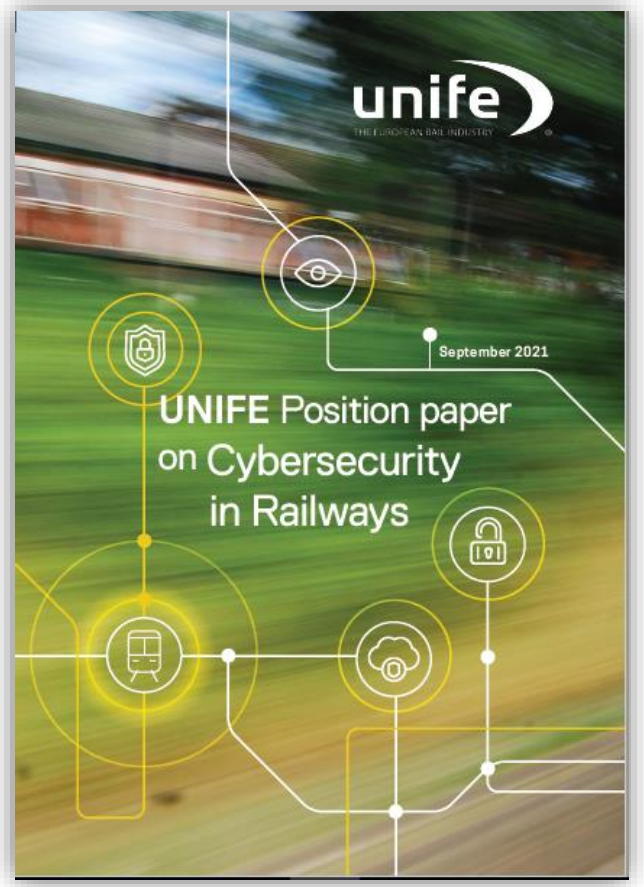
The European rail supply industry is **putting huge efforts to protect rail systems** from exploited cyber vulnerabilities, with different methods:

- **IEC 62443** - Security for Industrial Automation and Control Systems,
- **Major landmark** Its railway-specific adaptation **CENELEC CLC/TS 50701:2021** 'Railway applications – Cybersecurity' *CLC/TS 50701:2021, currently* being migrated to IEC 63452
- **Other major obligations** in the sector-specific regulation, supply chain requirements and contractual requirements.

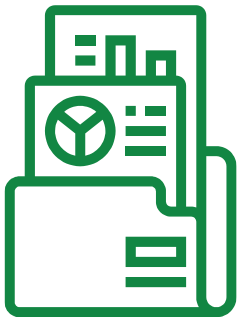
**UNIFE position paper on cybersecurity in railways is aimed at harmonising cybersecurity considering a sectoral approach across the European Union**

# Unife Position paper on Cybersecurity in Railways

September 2021



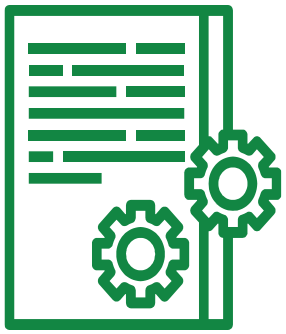
# Short-term challenges with high-priority (1/2)



01 Standardisation

**Major milestone: CLC/TS 50701 – Railway applications – Cybersecurity**

- As an example of a collaborative approach
- Awareness-raising among rail stakeholders in the TS50701 as the most promising way to harmonise requirements in the short-term, currently being migrated into an international standard.
- Build on the already well rolled-out IEC62443



02 Legislative Framework

**Legislative Framework**

- NIS2 Directive, Cyber Resilience Act proposal, Cybersecurity Act
- Horizontal approach shall ensure that there is not an overlapping
- Considering the particularities of the industrial sector is key to success in cybersecurity in railways

# Short-term challenges with high-priority (2/2)

03 Particularities of the rail sector

**Particularities of the rail sector to be considered when addressing cybersecurity**

- The sector's regulatory complexity – Including Operational Technologies (OT) in rail systems, that primarily interacts with the physical world.
- To ensure the interaction with the physical world, the rail sector has already its own regulation
- Legacy systems coexist with new systems
- Complexity of the value chain and interactions
- Rail is a system of sub-systems
- Long life-cycle of the rail products (over 30 years)
- Long life-cycle of the manufacturing process (up to 7 years)

# UNIFE position on the Cyber Resilience Act proposal

**UNIFE considers cybersecurity as a priority and believes that a coherent regulatory framework covering the cybersecurity of connected products is of utmost importance.**

- **It is critical to consider the particularities of different sectors**, especially industrial sectors, like for the rail sector, where a vertical approach is key to success in increasing the cyber resilience of products and systems.

- Higher overlapping risks with existing rail regulations, and a huge **financial impact on the European rail supply industry putting at risk its competitiveness**.

- It is important to avoid the setting-up of additional regulation in an **already highly regulated industry** where cybersecurity provisions can be integrated in the existing European rail regulation.

**The rail sector should be excluded from the scope of the CRA proposal.**

**UNIFE will release soon a position paper on the Cyber Resilience Act proposal**


See you soon

# THANK YOU

**www.unife.org**

**@UNIFE**

**UNIFE - The European Rail Supply Industry Association**

unife
THE EUROPEAN RAIL INDUSTRY ®