

## **UNIFE Cybersecurity Vision**

November 2023 ERA-ENISA Conference: Cybersecurity in railways, Athens Marta García Technical Affairs Manager

## **UNIFE – The European Rail Supply Industry Association**

#### What is UNIFE?

**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 <u>www.unife.org</u> or follow @unife on Twitter and LinkedIn.



### **Our Members and Associate Members**

GROUP RAILWAY SYSTEMS TEAM ABB C BONATRANS FREQUENTIS -----KONČAR ELTEC System Progress Rail SAFT ⇒mermec Končar - Electric Vehicles Inc A Carapillor Somaney АКЖА enyse ⊂4F CYLUS TELESTE VOITH funkwerk)) mermecste (h) HIRSCHMANN KONI PROLAN 🔕 SCHAEFFLER éolane ALSTOM D DAKO-CZ *<b>KTESMEC* camlin rail Gerflor HITACHI MOS ELETTRONICA # vession 🜔 kontron Promeco SCHEIDTHBACHMANN Inspire the Next ALTPRO िटहद 1 THALES GESTE HITACHI ABB 🔀 κονυχ Selectron 🗢 VŪKV PROVER *MIPRO* DELLNER ERICSSON cellnex Ardanuy DIGAS GHH-RADSATZ 1/2 LEONARDO neat triorail WALBO 44 HOPPECKE Radiall 🏹 ErvoCom SIEMENS G ti Duallnventive WENZEL ASTRA RALINGVATIO CENTRALP MITTCMARCON LiPPERT V7 evopro 🗟 ŠKODA NET MODULE ındra Unex EKE GREENBRIER LUCCHINIRS A)(TONE Ocomesvil EXPRESS RazorSecure NOKIA  $\sim$ SOFTIL **F** v d s Comtest Wireless elcowire rail\*\* masats Talgo HACON Faiveley Tomos oltis group REIOC BVV SEIT 1842 ELMA HARTING Kalthoff PILZ VIAVI **FOGTEC**\* MATISA 🍰 Constellium бТ Continental 3 TECHNE ÉLPA Bodet Megger. 🖏 Vibra*Tec* **Plasser**<sub>4</sub>Theurer S81 ISKRATEL HASLERiail **KNORR-BREMSE** FRAUSCHER ontiTech ASSIFER zvei **.**AGORIA R 5 Air ROMANIAN RAILWAY INDUSTRY ASSOCIATION **SWISSRAIL** Verband der DIE BAHNINDUSTRIE. RASTIA MAFEX AME I electrifying SWEDTRAIN

www.unife.org

## **Cybersecurity in railways**

#### Legislative framework: rail-relevant horizontal regulatory initiatives



- 1. Resilience, technological sovereignty and leadership
- 2. Building operational capacity to prevent, deter and respond
- 3. Advancing a global and open cyberspace through increased cooperation



- 1. A high common level of cybersecurity in the EU
- Complex architecture
- address the security of supply chains, reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements



In force since 2019

- 1. EU Cybersecurity Act grants a permanent mandate of ENISA
- 2. European cybersecurity certification framework for Information, communication and technology (ICT) products, services and processes



#### In force since 2019

- 1. Establishes a regulatory framework for placing radio equipment on the market
- 2. Harmonisation on radio equipment requirement

# EU Cyber Resilience Act

#### Proposal in sept. 2023:

- Cybersecurity by design in products, certification
- Reporting obligations when exploited vulnerabilities occur,
- Patch management,
- Important penalties

#### Other legislative initiatives addressing cybersecurity



**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





#### **UNIFE comparison vision in 2021** Short-term challenges with high-priority



The most promising way to harmonise cybersecurity in rail and to consider OT cybersecurity.

- TS 50701 and:
- Its international migration in IEC 63452

#### 01 Standardisation



Framework

Horizontal regulation shall consider the particularities of complex sectors and legal instruments should be sufficiently coordinated.

The need to research and innovation in cybersecurity in rail is a priority, especially considering the evolving threat landscape.

#### 04 Research & Innovation



Monitoring the latest trends in cybersecurity is key to ensure protection of our systems through new paths (e.g., supercomputing, blockchain, etc).

#### 05 Latest-trends



Rail sector is very complex and particular. Long-term vs agility:

- Legacy systems
- Vertical regulation
- Patch management allowance İS needed.

06 Particularities of the rail

sector www.unife.org





Cooperation is always essential, but specially it is in cybersecurity to fight against the cyber-criminals.

03 Cooperation

## And how is this vision now?

It is similar, but with a big challenge, the new Cyber Resilience Act legislative proposal
Unife Position paper on cyber

UNIFE position paper on cyber resilience in railways is aimed at highlighting the difficulties in implementing the CRA horizontal proposal in the rail sector, that would have a negative impact for the European rail supply industry







www.unife.org

## CRA in a nutshell (1/2)

Horizontal cybersecurity requirements for products with digital elements

## **Obligations of manufacturers**

Assessment of the risks associated with a product

(1) Product-related essential requirements (Annex I, Section 1)
(2) Vulnerability handling essential requirements (Annex 1, Section 2)
(3) Technical file, including information and instructions for use (Annex II + V)



Reporting

obligations

to continue

Conformity assessment, CE marking, EU Declaration of Conformity (Annex IV)

Continued compliance with **vulnerability handling** essential requirements throughout the product life time (Annex I, Section 2)

Design and development phase Maintenance phase (5 years or across product lifetime, whichever is shorter)

Obligation to report to ENISA within 24 hours:

(1) exploited vulnerabilities

(2) incidents having an impact on the security of the product



Source: European Commission

## CRA in a nutshell (2/2)

1

3

4

5

6

#### Horizontal cybersecurity requirements for products with digital elements

Affecting all connected products/software with digitals elements

EU Cyber Resilience Act

For safer & more secure digital products



2 Requirements to include cybersecurity by design (through standards, standardisation request)

Certification of the products, depending on the criticality (self-assessment/third party assessment) **CE marking** 

Management of the exploited vulnerabilities (patch management) including reporting obligations

Most of the responsibilities relies on the manufacturers

Penalties for not being compliant with this regulation are very high



## Focus on the main challenges of CRA for the rail supply industry

## Cybersecurity by design

Cybersecurity by design will be introduced in all the products/software with digital elements placed on the market (Annex I section 1)

- According to the relevant standards
- Certification, self-assessment, third party assessment

### Patch management for free

Exploited vulnerabilities will have to be reported, and patches for those vulnerabilities will need to be delivered by the manufacturer for free

• Period: likely to be during the lifetime of the product

## Standardisation request

The CRA's proposes a standardisation request, horizontal standard that will cover all sectors (ICT and OT)

- When possible, based on existing standards
- UNIFE believes that differentiation between ICT and OT should be considered (2 standards applicable)



### Focus on the main challenges of CRA for the rail supply industry – What would it mean for the rail sector?



More certification is needed.

of their processes,

Costs will increase, which can be seen as an investment to protect the products



these costs when they make offers, which will be extremely difficult and may prevent suppliers from submitting offers.

Overall, it is evident that the financial impact on the rail sector will be significant



standards for rail are the ones used in the CRA standardisation request:

- IEC 62443 series that is the baseline for
- TS 50701
- Upcoming IEC 63452

Where a huge work and cooperation has been/is being done and because are the only option for rail OT.

## Conclusions

- Horizontal regulation must consider the particularities of complex sectors, especially those ones having Operational Technologies and considered critical under the NIS2 → Important to consult the rail sector at the right time!
- 2. Legal instruments must be sufficiently coordinated
  - 1. E.g., CRA and Cybersecurity act implementing regulation
- **3.** Horizontal and vertical regulation must be very well coordinated avoiding overlapping, that may lead to a burden for the companies, higher increase of the costs, etc.
- 4. The applicable standards for all the new and upcoming legislation must consider the sector specific standards (even if the regulation applies to very different sectors)
- 5. Certification schemes for rail must consider OT, instead of ICT products
- 6. Collaboration is essential and key to enhance cybersecurity and cyber-resilience, rail manufacturers have been, and are willing to cooperate with stakeholders to improve cybersecurity in rail



## **CYBER SECURITY**

## See you soon **THANK YOU**

www.unife.org



UNIFE - The European Rail Supply Industry Association

