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 www.unife.org or follow @unife on Twitter and LinkedIn.

www.unife.org

Our Members and Associate Members

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**

Proposal in sept. 2023:

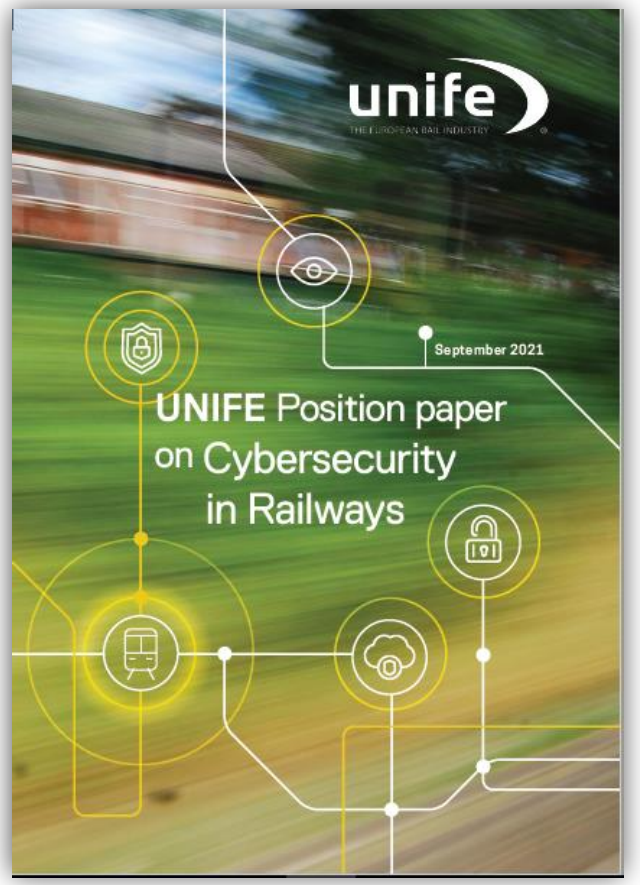
- Cybersecurity by design in products, certification
- Reporting obligations when exploited vulnerabilities occur,
- Patch management,
- Important penalties

Other legislative initiatives addressing cybersecurity

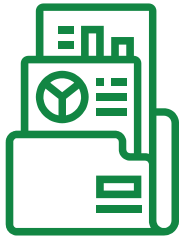
UNIFE position paper on cybersecurity in railways is aimed at harmonising cybersecurity considering a sectoral approach across the European Union

Unife Position paper on Cybersecurity in Railways

September 2021



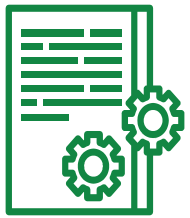
UNIFE comparison vision in 2021
Short-term challenges with high-priority



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



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

02 Legislative Framework

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

03 Cooperation

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 is needed.

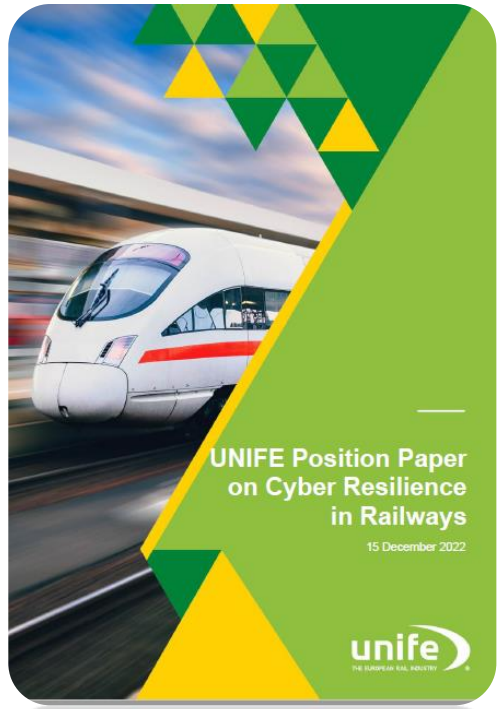
06 Particularities of the rail sector

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 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

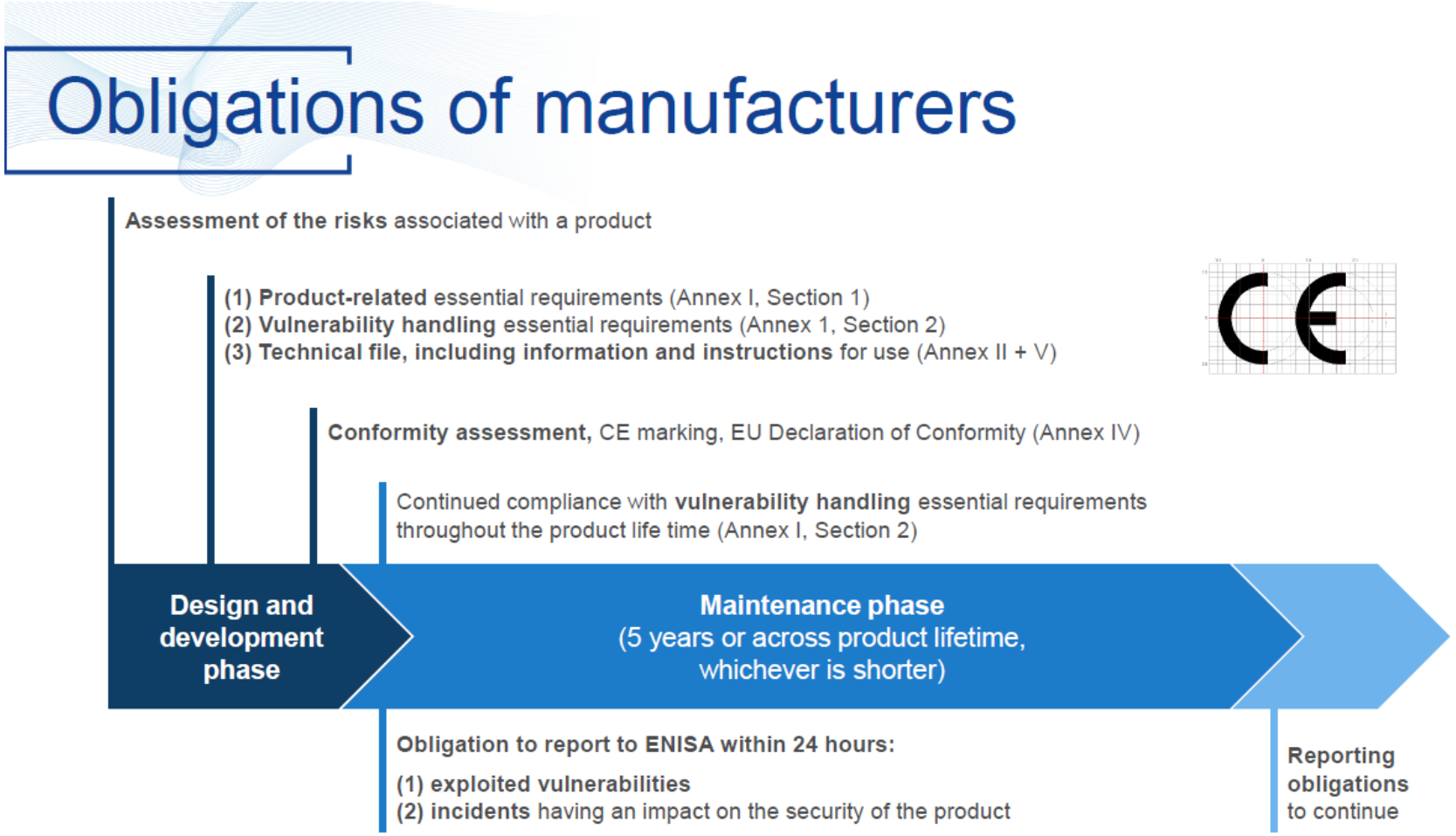
Unife Position paper on cyber resilience in Railways



December 2022

CRA in a nutshell (1/2)

Horizontal cybersecurity requirements for products with digital elements



Source: European Commission

CRA in a nutshell (2/2)

Horizontal cybersecurity requirements for products with digital elements

1. Affecting all connected products/software with digitals elements
2. Requirements to include cybersecurity by design (through standards, standardisation request)
3. Certification of the products, depending on the criticality (self-assessment/third party assessment) **CE marking**
4. Management of the exploited vulnerabilities (patch management) including reporting obligations
5. Most of the responsibilities relies on the manufacturers
6. Penalties for not being compliant with this regulation are very high

unife
THE EUROPEAN RAIL INDUSTRY

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)

unife
THE EUROPEAN RAIL INDUSTRY

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

SHARP COSTS INCREASE

Cybersecurity by design

Including cybersecurity by design means that:

- Manufacturers will have to proceed with the re-engineering of their processes,
- More certification is needed,
- Costs will increase, which can be seen as an investment to protect the products

Patch management for free

Costs are **nearly impossible to estimate** (systems are custom build, long lifetime over 30 years). Rail suppliers will have to factor in 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

Standardisation request

The rail supply industry needs that the applicable 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.

unife
THE EUROPEAN RAIL INDUSTRY

Conclusions

1. **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**

unife
THE EUROPEAN RAIL INDUSTRY

See you soon

THANK YOU

www.unife.org

@UNIFE

UNIFE - The European Rail Supply Industry Association

unife
THE EUROPEAN RAIL INDUSTRY ®