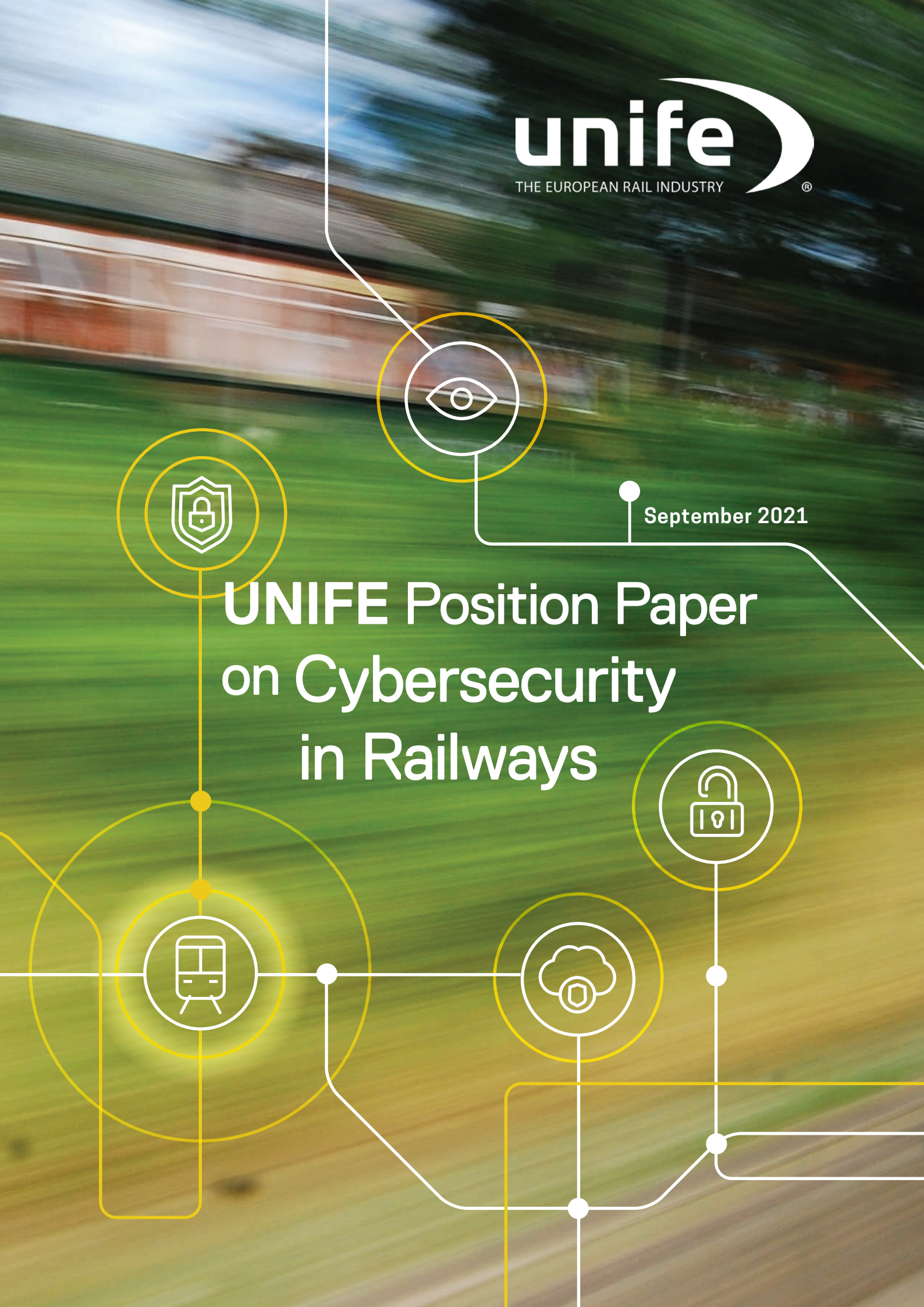

unife
THE EUROPEAN RAIL INDUSTRY
September 2021
UNIFE Position Paper
on Cybersecurity
in Railways

CONTENT

ABOUT UNIFE

Based in Brussels since 1992, UNIFE is the association representing Europe's rail supply industry at the European Union (EU) and international levels. UNIFE's members include more than 100 companies – from SMEs to large industrial players – active in the design, engineering and manufacture of rolling stock (i.e., trains, metros, trams, freight wagons) as well as rail signalling and infrastructure equipment. UNIFE also brings together the national rail industry associations of 11 European countries.

The rail supply industry, a key player for economic growth and industrial leadership

Providing 400.000 jobs, reaching €47 billion in combined annual sales and generating increased environmental excellence of the products they manufacture and sell all over the world, European train-builders and rail equipment suppliers have been a key contributor to the competitiveness and sustainability of the EU's industry.

Rail, an essential component of the EU Green Deal

The **EU Green Deal** sets Europe's path to climate-neutrality by 2050. No such goal can be fulfilled without the decarbonisation of the transport sector, which accounts for nearly a quarter of all European emissions. Rail stands as the exception – having steadily reduced its carbon footprint for the past two decades, while improving its energy efficiency. As the most sustainable form of mass transportation available, it must be a critical component in the EU's plan to actualise its aspiration to connect all of its regions in the most climate-friendly manner.

INTRODUCTION

This cybersecurity vision, developed by UNIFE, presents the European rail supply industry's assessment of challenges to securing Europe's railway system as it continues to incorporate digital innovation across its assets. This examination also aims to set priorities and targets for the short-, medium- and long-term. A set of recommendations is also proposed to further engage with the EU institutions and other rail stakeholders.

BACKGROUND

Cybersecurity: a priority for the European rail supply industry

The European rail supply industry recognises that mitigating cyber-threats is vital to maintaining a safe, reliable railway and urban rail public transport. This is no small feat given their complex interdependences and legacy infrastructure elements. Cybersecurity is a key requirement to enable these mobility systems to effectively deploy and fully leverage a connected, digital environment. Ensuring the integrity of both mainline and urban rail transport systems and maintaining operational continuity standards is an objective which is shared by the whole sector.

Cybersecurity threats are usually cross-border, and a cyber-attack on the critical infrastructure of one country can easily affect the whole EU. Consequently, Member States need to have strong government bodies in place, capable of conducting cybersecurity measures in their own territory, as well as collaborating with their counterparts in other Member States by sharing information. This is particularly important for sectors that are critical to the normal, uninterrupted activity of society[1]. Rail is considered a critical sector due to the risks associated with transporting essential passengers and goods and the vast system's high reliance on telecommunication networks.

Policy and regulatory framework

The establishment of an *EU Digital Single Market Strategy* is expected to harmonise processes and solutions once the new or revised cybersecurity legislation is introduced.

However, the rail sector faces a complex regulatory framework that requires a deep understanding of all operational cybersecurity-related processes. Furthermore, digitalisation has transformed rail transport, notably from the operational, infrastructural, and mass-transit perspectives. It has also furthered the potential for interoperability. Therefore, the implementation of cybersecurity requirements is fundamental for the sector's digital enhancement and security.

At the EU level, the cybersecurity's policy and legislative frameworks are changing at a regular pace and several initiatives have been launched to address a more coherent and harmonised cybersecurity management regime across Europe. Chief among those initiatives are the *General Data Protection Regulation* (GDPR), the *Cybersecurity Act,* and the *EU Cybersecurity Strategy.* The last document, as well as the most important one, is composed of the *Network and Information Security Directive* (NIS2) revision and the *Resilience of Critical Entities Directive.* Those requirements are applicable to the specific regulatory landscape of railways, as specific actions such as increasing the resilience of the **European Railway Traffic Management System** (ERTMS) and further introduction of **telematics applications for freight and passenger services** (TAF/TAP) in data and messages exchange within the TSIs revision by 2022.

All new cybersecurity policy and regulatory proposals constitute a *New Legislative Framework,* a positive contribution towards harmonised processes which could prove challenging as national level implementation could increase the complexity of complying with the timeline and regulations.

1 EU Digital Strategy: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

The challenge of cybersecurity for the European rail supply industry

In addition to the policy and regulatory framework, cybersecurity is also a potential liability for companies responsible for Information and Communication Technology (ICT) products and services, as their resiliency involves all stakeholders along the value chain.

The speed at which cybersecurity solutions are launched and implemented is closely linked to both private and public resources. These are allocated by the European actors ranging from as public entities and authorities to private companies to ensure a swift and comprehensive deployment of new technologies and services to prevent or combat cyber-crime.

Currently, all decarbonisation projects are linked to a smart digitalisation strategy. Cybersecurity cost impact should be considered as part of the investment to protect and secure digitised critical infrastructure.

It is well understood that the cybersecurity environment is constantly evolving. The degree of existing cyber-resiliency is a culmination of the whole system's individual critical business assets, the threat landscape, and the maturity of available cyber capabilities. All of these must be considered and lead to integrating customised cybersecurity awareness and actionable measures for an operational, managerial and executive purpose.

There are multiple avenues to create a solid baseline for cybersecurity harmonisation within Europe's rail sector:

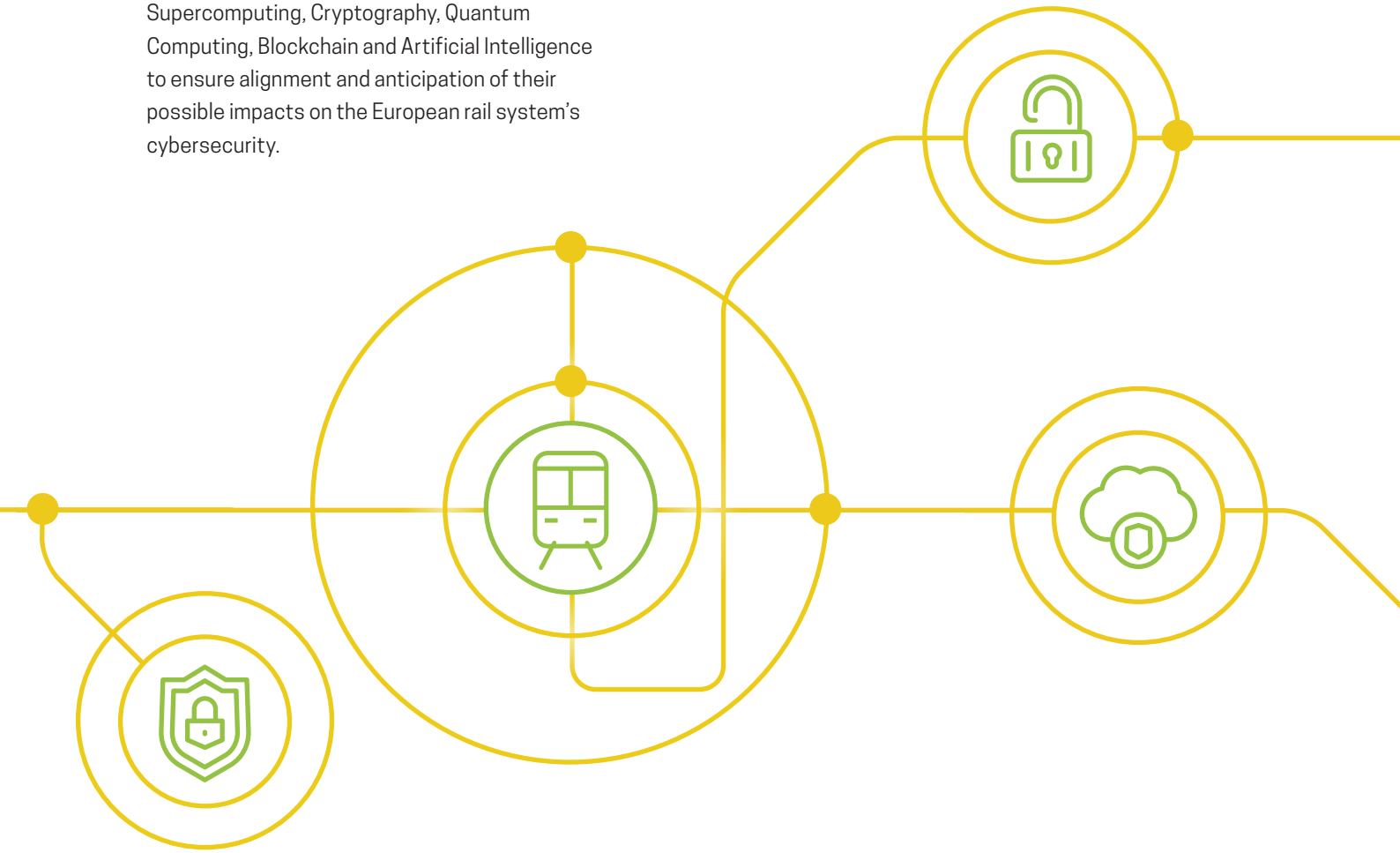
1. **Standardisation at the EU level via CENELEC: CENELEC TC 9X** has tasked Working Group 26 with publishing a Technical Specification *(CLC/TS 50 701)* that has already been published in July 2021, that addresses the application of the widely accepted *IEC 62443 standard "Security for industrial automation and control systems"* to rail sector. The *"CLC/TS 50701:2021 Railway applications – Cybersecurity"* will be a key milestone for the rail sector as it is applicable to all of its sub-systems, including rolling stock, signalling and infrastructure.
2. **Legal framework at EU level:** Europe has prioritised legislation addressing new technologies vital to the Union's digital transition. Several regulatory initiatives already focus on cybersecurity as a cornerstone of efforts to protect networkable products and services. Ensuring regulatory coherence should be a key objective of the *Network and Information Security Directive* (NIS2) revision, especially as it is envisaged to extend its scope. Concurrent legislative proposals aim at reducing fragmentation among Member States while building our collective cybersecurity resilience. However, horizontal and sectoral legal instruments should be sufficiently coordinated and possible regulatory overlaps should be avoided. To this end, sufficient coordination between the relevant NIS2 provisions and sector-specific legislation must be promoted.
3. **Cooperation within the rail sector:** UNIFE plays an important role as the rapporteur of the European Rail Supply Industry's cybersecurity vision. The association facilitates dialogue between companies through the activities of its Cybersecurity Working Group. Additionally, following the creation of a *Digitisation Rail Roundtable* in early 2019 by **DG CONNECT** and **DG MOVE** to discuss rail sector digitisation/digitalisation priorities, UNIFE coordinated a cybersecurity workstream that brought together experts from across the rail sector. Starting with an analysis of ongoing rail sector cybersecurity legislation initiatives at both the EU and national levels, the current standardisation & regulation environment, and Research & Innovation (R&I) activities, this collective effort resulted in our sector presenting four key recommendations to the **European Commission.**

Cooperation from across the sector and with EU institutions is key to achieving homogenous results that draw on lessons learned to protect the European Rail Sector.

4. **Research & Innovation (R&I):** Transversal cooperation on cybersecurity through the participation in EU funded R&I projects - including future ones under **Horizon Europe** and within the future **Europe's Rail Joint Undertaking** (ER JU). It is important to mention that past and ongoing rail R&I projects have already addressed elements of rail cybersecurity. For instance, **Shift2Rail Joint Undertaking** (S2R JU) projects like Roll2Rail, CONNECTA and X2Rail projects completed work on Train Control and Monitoring Systems (TCMS) and cybersecurity. 4SECURail has also developed a **Cyber Security Incident Response Team** (CSIRT) model for the rail sector with successful outcomes. All of these examples and initiatives show the importance of cooperative Research and Innovation projects for our collective security. Considering the continued emergence of cyber-threats, similar transversal cooperation is expected in the form of future projects under Horizon Europe and the future ER JU.

5. **Monitoring of the latest trends:** Rail must continue to be aware of major technological advancements in key fields such as Supercomputing, Cryptography, Quantum Computing, Blockchain and Artificial Intelligence to ensure alignment and anticipation of their possible impacts on the European rail system's cybersecurity.

6. **Specific particularities of the rail sector - Legacy Systems:** Rail stakeholders need to balance operational needs, business competitiveness, implementation of new technologies and cybersecurity as the rail sector undergoes a digital transformation that increases the risk of cyber-attacks. The sector's regulatory complexity makes Operational Technologies (OT) in rail systems quickly obsolete or outdated as they are based on what is considered a secured approach at the time of conception but is easily bypassed once the technology that underwrites it is eclipsed. This makes difficult to keep implemented OT Systems compliant with up-to-date cybersecurity requirements. Furthermore, the different locations of those systems - typically distributed throughout the network at the stations, along tracks and more across a country and on mobile assets such as the rolling stock and in onboard equipment - make comprehensive cybersecurity controls difficult. Considering cybersecurity when drafting new railway regulations allows for more consistent review of the sector's needs.



CHALLENGES FOR THE EUROPEAN RAIL SECTOR

Short-term challenges with high priority 1→3 years

STANDARDISATION AND REGULATION TOPICS

The Technical Specification CLC / TS 50701 developed in CENELEC TC 9X WG 26 must be considered as certification scheme for the rail sector

The European Union Agency for Cybersecurity (ENISA), is now mandated, as established under the *Cybersecurity Act 2019/881,* to work on the development of a European cybersecurity certification framework for technology (ICT) products, processes and services. Each scheme will specify one or more levels of assurance (i.e., basic, substantial or high), based on the level of risk associated with the envisioned use of the product, service or process. The proposed framework will ensure that connected products and products manufactured in, or for, the EU market that - in some cases - are capable of plugging into the internet of things (IoT) will be developed with cybersecurity measures in-mind from the design stage – or are created using "security by design" thinking. If necessary, the rail sector will have to agree on the specific critical ICT services, systems or products that may be subject to certification, and the type of certification to be certified with regard to security.

Within the rail sector, the CENELEC TC 9X/WG 26 has developed the *"CLC/TS 50701 Railway applications – Cybersecurity"*, notably covering signalling, rolling stock and fixed installation. The new CLC/TS 50701 should serve as the basis to create a homogenous certification scheme for rail ICT products, services, and processes.

This is the most promising way to rectify short-term obstacles. A Technical Specification (TS) for handling cybersecurity in a unified way for the whole rail sector could fulfil this need, considering that it is based on an already existing Industrial cybersecurity standards (e.g., IEC 62443).

The CLC/TS must be rolled out within companies. Initially, it will be implemented on a project basis, while the long-term goal is to reach a state in which processes, including a risk-based approach addressing potential threats, are certified. Data related to the applicability of the TS will be collected and documented, as well as a roadmap to gradually adapt projects to the CLS/TS considered.

Lastly, once the standard is ready, it must be decided if a certified body is needed. In that case, its relationship with the safety authorisation process - which has moved from the national authorities to the **European Union Agency for Railways** (ERA), thanks to the Technical Pillar of the 4th Railway Package - must be coordinated. This must be a harmonised, adequate and aligned approach that meets the different necessities of safety and security.

Awareness-raising among rail stakeholders in the CLC/TS 50701

As mentioned in the section above, the challenges specific to the rail sector need to be addressed in the short term and with a homogeneous starting point. To tackle this properly, raising awareness of all EU rail stakeholders on the minimum criteria set out in CLC/TS 50701 is of particular importance. This will allow the European rail sector to know and correctly apply these criteria in the same way across the rail network.

This should be done not only in a horizontal approach that considers all rail industries, but also in a vertical approach which accounts for all staff contributing to our sector's cybersecurity.

To achieve this, workshops and trainings should be held within the rail sector to take this approach into account and provide it with a common framework for gathering a minimum set of cybersecurity requirements.

Promotion and migration the CLC/TS 50701 into an International Standard

The CENELEC CLC/TS mentioned above needs to migrate to the **International Electrotechnical Commission** (IEC) with the aim of having an international standard based on it. This process could take 6 years.

Market access as a result of increased competitiveness and efficiency, reduced trading costs, simplified contractual agreements and increased quality would be achieved if this was to occur.

Convergence of CENELEC Standardisation and EU R&I project (e.g., the future Europe's Rail Joint Undertaking, Horizon Europe)

There must be a strong cooperation between CENELEC and EU R&I initiatives within Horizon Europe such as Europe's Rail Joint Undertaking. The results achieved by EU R&I initiatives can be used later for the development of new European standards. Potential issues identified in standardisation activities could inspire the development of new rail research topics. This cooperation must be reinforced.

UNIFE position on cybersecurity in preparation of the next CCS TSI and ensuring it is appropriately addressed in new and existing TSI

Concerning the Control Command and Signalling (CCS) TSI, UNIFE (via **UNISIG**) is actively involved in the development of the future ERTMS game changers, in coordination with Shift2Rail Innovation Programme 2 and ERA coordination groups dealing with the system. The most important enablers are **Automatic Train Operations** (ATO), ERTMS Level 3, **Future Railway Mobile Communication System** (FRMCS) and cybersecurity. Concerning the latter, the main aim is to achieve the optimal level of protection against any significant threat to the signalling and telecom systems that Europe relies on in the most economical way.

Notably, under the revised CCS TSI 2022, ERA and rail sector organisations will both evaluate the level of protection provided by the current ERTMS specifications and prepare them for additional requirements linked to the game changers' introduction - mainly, 5G-based FRMCS.

Additionally, cybersecurity must be addressed appropriately in the development of new and revision of existing TSI, such as the CCS and TAF/TAP TSI.

UNIFE is advocating for the following future security design and cost criteria to be applied: strong protection of data integrity (safety), availability (operational performance) and confidentiality - protecting credentials. Interoperability, backward compatibility (long-term migration) and the use of standard technologies will ensure maintainability and upgradability. Conversely, inter-system interdependency and unnecessary complexity should be avoided. The cost of implementation and operation for (re)certification and homologation must also be kept low.

LEGISLATIVE AND POLICY FRAMEWORK

Consistency in the New Legislative Framework

The political and legal framework is changing rapidly to meet the opportunities and challenges Europe is facing through increasing digitalisation and therefore the level on cybersecurity. There are several legislative initiatives dealing with cybersecurity, above mentioned, considered in the policy and legislative framework.

Although the above legislative initiatives may address legitimate cybersecurity concerns, they need to be coordinated so as not to lead to regulatory fragmentation with overlapping and conflicting requirements for European rail stakeholders. The introduction of horizontal cybersecurity legislation for networkable products within the new regulatory framework with good coordination would be very effective and beneficial to increase cybersecurity.

COOPERATION AMONG RAIL STAKEHOLDERS

Establishing good cooperation among rail stakeholders and the Information Sharing and Analysis Centre (ISAC)

Cybersecurity knows no borders, neither do cyber-attacks. All rail stakeholders need to work together to keep abreast of the latest threats affecting the sector both within the European Union and at the global level.

Information Sharing and Analysis Centre (ISAC) initiatives are promoted by the Commission and ENISA. Through such platforms, a **European Rail -Information Sharing and Analysis Centre** (ER -ISAC) – is open to rail stakeholders from all EU member states. UNIFE supports the activities of ER -ISAC and is willing to maintain an open and positive dialogue to improve the exchange of information between disparate elements within the rail ecosystem. Nevertheless, collaboration and sharing should take into consideration the NIS2 Directive proposal regarding the new categories of "essential entities" and "important entities", including in the specific case of the rail sector the infrastructure managers, railway undertakings and the rail supply industry.

The aim of such a platform should be to provide a central resource for the collection of information on cyber-threats, particularly those concerning critical infrastructure. It also should enable the mutual exchange of information between the private and public sectors on the root causes, incidents, and emerging threats. It should also facilitate the sharing of experiences and best practices, knowledge, and analysis. Such a structure that leverages close cooperation is key to improving the sector's cybersecurity readiness and awareness.

CYBERSECURITY ALONG THE RAIL SUPPLY INDUSTRY

Ensure an adequate level of rail supply cybersecurity at EU and National levels with a common approach

The European rail supply industry is only truly secure when all its components carry out effective, coordinated security measures with the shared objective to ensure the integrity of supply chain data and the safety of products – helping to contribute to the security of the global economy.

New obligations were generated by the New Cybersecurity Regulatory Framework. Among them is ensuring the correct security assessment along the supply chain – according to the NIS2 Directive proposal – which introduces several requirements to conduct supply chain security assessments. It is crucial that these assessments stay risk based and non-discriminatory, allowing a competitive and harmonised single market with coordinated Member State approaches.

Together with rolling out the process, as described in the CLC/TS 50701, it is important to secure the entire rail supply chain. The implementation of security targets only works if rail suppliers are involved in cybersecurity assessments and know how to create secure products and subsystems.

The objective is ensuring the correct level of cybersecurity along the rail supply chain through a homogenous approach. Fewer resources would be needed for, and costs incurred by companies to comply with the cybersecurity framework requirement.

UNIFE members can contribute to implementing security features and processes across completed rail systems. However, these criteria often start with a vertical approach. Consequently, to have a common risk assessment framework, the cooperation of the entire railway sector is necessary.

RESEARCH & INNOVATION

Increase Research & Innovation investment for cybersecurity

Cyber-threats continue to accelerate and are evolving fast, yet the stream of new and effective cyber-defence technologies has grown much more slowly. The gap between threat and defence has widened, as cyber-criminals deploy increasingly sophisticated offensive technology and engage in cyber-crime with unprecedented power, resources, and global reach.

Against this backdrop, there is a need to shorten "time to market" to release rapidly innovative cyber-defence concepts.

Adapted methods and strategies against ever-evolving cyber-threats should be developed in a way that goes beyond state-of-art of cybersecurity and be able to anticipate such cyber-threats. Consequently, more investment in Research & Innovation is needed to support the development of new defence methods strategies through collaborative research between

different European rail stakeholders. The future Europe's Rail Joint Undertaking, under Horizon Europe, will be a key avenue to developing these competencies.

PARTICULARITIES IN CYBERSECURITY WITHIN THE RAIL SECTOR

Considering cryptography as one pillar of Cybersecurity

Cryptography plays a vital role in ensuring confidentiality, integrity, and authentication. Weaking cryptography with backdoors [2], for example, is a very dangerous path that would lead to less secure systems. Beyond end-to-end encryption, and encrypting data at rest, we also recommend having appropriate cryptographic code signing mechanisms and the associated validation infrastructure. Additionally, it is important to be prepared for the rapid deployment of expected new standards for postquantum digital signatures and crypto agility in products.

Railway Legacy Systems will be evaluated with an adequate risk acceptance assessment

The European rail sector manages many legacy systems. Some were designated obsolete by the New Legislative Framework. For example, some signalling and rolling stock was classified as such as its lifespan is calculated in decades. To comply with the new cybersecurity measures, an adequate risk acceptance scheme and assessment for legacy systems is needed.

This could lead to refurbishment programmes that may include provisions for attack detection systems as a compensation countermeasure. This would require high levels of investments to refurbish those systems.

There is also the possibility of creating a different certification scheme for those legacy systems. This could be implemented by accepting a minimum of vulnerability assessment.

For the new products and services, lifecycle management that includes cybersecurity and countermeasures should be planned and anticipated for new systems, as established in the CLC/TS 50701.

Improve rail maintenance in secure conditions – by setting up an allowed patch management

The organisational and technical measures needed to maintain an acceptable degree of cybersecurity along the system's whole lifetime are very relevant for our sector. OT systems in rail are often based on parameters which used to be secure at the time when they were installed but, due to the long-life cycle of those systems, have become obsolete or outdated from a cybersecurity perspective.

As cyber-threats rapidly evolve, a system may no longer be secure in a short period of time. These assets must be permanently secured, with the correct implementation of the patch's management in an agile manner. This is a challenge for the sector, as any change - no matter how significant - must be subject to analysis and certification when applicable. This seems difficult to reconcile with the time needed to analyse the impact of the change on railway safety.

The main challenge is to successfully define patch management processes that allow agile and streamlined maintenance in secure conditions that do not impede the safety of such system.

Mid-term challenges 4→6 years

Quantum-Secure and Crypto-Agility

As quantum technology becomes more sophisticated, it will increasingly jeopardise the security and strength of the public key cryptographic paradigm. If sufficiently large quantum computers can be built, they will be able to break specific public key cryptography [3] and asymmetric cryptography [4] that underpin the existing infrastructure and networks.

The European rail supply industry needs to make its IT infrastructure *"Quantum-Secure"* before large-scale quantum computers become readily available. Protecting data will involve implementing quantum-resistant algorithms (Post-Quantum Cryptography), in the short term, on existing classical computers and re-encrypting data.

2 Backdoor refers to any method by which authorised and unauthorised users are able to get around normal security measures and gain high-level user access.

3 Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it.

4 Asymmetric cryptography is a second form of cryptography. Asymmetric cryptography is scalable for use in very large and ever-expanding environments where data are frequently exchanged between different communication partners.

Development of technologies to secure multimodal mobility

Digitalisation is set to be a driver for multimodal transport, in which travel by air, rail, road and sea will be integrated. This will require the integration of the different IT and OT systems and harmonisation of their respective cybersecurity methods. There is ongoing research on this topic within S2R JU today, to provide sustainable, smart, multimodal transport by employing V2X and 5G communication technologies. This research must be continued in the future ER JU.

From a regulatory and standardisation perspective, different transport modes and their OT systems have their own standards and certifications. However, the IT systems or cloud providers that are necessary to operate those OT systems will converge as we increase our multimodality capabilities. In this scenario, it is essential that all systems are covered under a corresponding legislative framework, aligned with the NIS2 Directive proposal.

Inclusion of strong cybersecurity criteria into all new technologies implemented in rail – for a more secure system in the near future

As we continue to carry out the digital revolution, new-age and disruptive technologies have created a new path for transformation. Some of the most influential emerging technologies are Artificial Intelligence, Smart Maintenance, IoT and Digital Twins. These, amongst others, promise to make operations future-ready in rail. Such technologies require huge amounts of data and should be subject to strong cybersecurity criteria. In particular, as Artificial Intelligence is increasingly beingly adopted across the rail sector, it can also be leveraged to improve the overall security. This is especially important in the present environment in which there is a constant threat of unforeseeable and highly sophisticated cyber-attacks. Intelligent security could be a more effective answer than human vigilance to the continuously evolving threat of intelligent malware.

When it comes to Blockchain technology, its fundamental attribute is the security it offers through its encryption and decentralised data storage. This can prove transformative for cloud infrastructure, as companies can safely move their mission critical processes to this digital ledger, perform required computations and update the data from time-to-time.

New disruptive technologies will aim at improving cybersecurity by upgrading a systems' level of defence, including those new technologies with solid and strong cybersecurity criteria and GDPR compliance.

Long-term challenges to be monitored for next priorities → beyond 6 years

Authorisation of processes, and not projects

In the initial phase of establishing the regulation process, it is inevitable that projects will be certified using the CLC/TS 50701. However, once rail manufacturers, infrastructure managers and railway undertakings have undergone the authorisation a few times, it will be more effective to certify the industrial development processes instead of each project separately.

Securing the entire product's lifecycle for next generation systems

Due to the long lifecycle of railway development, the regulation process utilised in initial projects will be applied to ongoing projects. In the long term, all projects will be developed using the CLC/TS methods from the beginning.

Increase such cross-sectorial cooperation – to vastly improve cybersecurity responses

As cyber-threats become more complicated, global collaboration will be even more critical for cybersecurity. A cross-sectoral cooperation framework, especially between different critical infrastructure sectors, is highly relevant. Sharing knowledge about threats, risks, vulnerabilities, and successful mitigation tactics would be very important for understanding and analysing the global landscape.

Building strong collaborative relations between different sectors should be fostered to bolster Europe's ability to confront cybersecurity challenges.

KEY MESSAGES AND RECOMMENDATIONS

UNIFE believes that to reach full cooperation in the European cybersecurity arena, there must be a collaborative approach that includes all necessary rail stakeholders in standardisation, R&I, and cyber-threats sharing activities. To achieve these ends, UNIFE calls on:

1) The European Commission (DG RTD, DG MOVE, DG CONNECT):

- To ensure regulatory consistency as a key objective of the NIS 2, given the envisaged scope expansion and concurrent legislative proposals on cybersecurity. Horizontal and sectoral legal instruments should be sufficiently aligned, and regulatory overlaps should be avoided. The NIS 2 should include clear jurisdiction rules for all entities that fall under its scope. This is essential to avoid ambiguity as to which Member State is allowed to enforce the obligations.
- To allocate more EU funding for railway research and innovation to ensure that cybersecurity is properly addressed, as it requires constant innovation to keep up with evolving threats. This is particularly important for the future Europe's Rail Joint Undertaking. The programme should address rail cybersecurity priorities and continue the work started in Shift2Rail and others European rail research projects.
- To allocate an adequate budget to ENISA, to allow it to play an important role in supporting the protection of critical infrastructures.

2) The European Agency for Cybersecurity (ENISA)

- To continue to considering railways in its cybersecurity strategy.
- To create the certification scheme for railways based in the CLC/TS50701, avoiding different criteria for cybersecurity implementation across Europe's rail sector.
- To provide further support to critical entities leading the EU effort to understand and manage cyber and physical risk to the critical infrastructure by creating a secure and resilient critical infrastructure for citizens.

3) The European Commission (DG CONNECT) and ENISA

- The NIS2 proposal introduces a number of requirements for conducting security assessments along the supply chain for particular products and services. It is, therefore, crucial that these assessments are risk-based and non-discriminatory to ensure a competitive and harmonised single market, with coordinated approaches across the Member States. Targeted rail sector companies should be involved in such risk assessments, as their expertise is fundamental to a successful consideration of complex rail supply processes.

4) The European Union Agency for Railways (ERA) and ENISA

- To continue their cooperation to strengthen cybersecurity in railways.

5) The European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC)

- To support rail stakeholders in raising awareness in Cybersecurity, especially through the new CLC/TS 50701.

UNIFE – The European Rail Supply Industry Association

Avenue Louise 221
B-1050 Brussels, Belgium
Tel: +32 2 626 12 60
general@unife.org

@UNIFE

UNIFE -The European Rail Supply Industry Association

www.unife.org