Promoting Rail Market Growth for Sustainable Mobility

UNIFE Vision on Cyber-Security in Railways

June 2020

UNIFE - THE EUROPEAN RAIL SUPPLY INDUSTRY ASSOCIATION
ww.unife.org
@UNIFE
UNIFE

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 major industrial champions– 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.

Introduction

This vision, developed by the UNIFE Cyber-security Working Group, presents the European rail supply industry assessment of challenges posed by cyber-securing Europe's railway system and aims to set priorities and targets for the short-, medium- and long-term. These will serve as the basis for further engagements with the EU institutions and the other rail stakeholders.

Background

Cyber-security is gaining importance across society. Cyber-security issues now frequently finds its way to the forefront of the news cycle, perhaps most notably was the WannaCry ransomware attack. Lawmakers all over the world reacted to the breach by enacting new legislation mandating operators, but also manufacturers, of critical infrastructure to take appropriate steps to protect their assets. In the EU, several initiatives have been launched to prioritise cyber-security within the EU agenda. The Network and Information Security (NIS) Directive 2016/1148, the Cybersecurity Act 2019/881 and the EU General Data Protection Regulation 2016/679 are Europe's most relevant steps towards a more coherent and harmonised cyber-security management regime.

Outside of legislative circles, cyber-security is also posing liabilities for companies responsible for the potential vulnerabilities of their products and systems.

The Digital Single Market Strategy of the EU is tasked with establishing harmonised processes and solutions when formulating the cyber-security legislation.

Furthermore, the speed at which cyber-security solutions are launched and implemented is closely linked to both private and public resources allocated by the main European actors to ensure a fast and comprehensive deployment of new technologies and services to prevent or fight cyber-crime.

There are multiple avenues to constructing such a harmonisation:

1) **Standardisation at the EU-level via CENELEC**: CENELEC TC 9X has tasked the Working Group 26 with publishing a Technical Specification (CLC/TS 50 701) by early 2021 addressing applying the widely accepted IEC 62443 standard "*Security for industrial automation and control systems"* to railway sector activities.

2) **Cooperation within the rail sector:** UNIFE plays an important role as a collector of the European Rail Supply Industry's cyber vision. The association facilitates dialogue between companies through the activities of its cyber-security 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 cyber-security workstream bringing together experts from across the rail sector. Starting with an analysis of ongoing rail sector cyber-security initiatives in the legislative field at both the EU and national levels, the current standardisation & regulation environment, and Research & Innovation (R&I) activities, this collective effort resulted in the development of four key recommendations from the rail sector as a whole to the European Commission.
3) **Research & Development & Innovation (R&D&I):** Transversal cooperation across sectors through the participation in EU funded R&D&I projects, including those under Horizon2020 and Shift2Rail. It is important to mention projects such as Roll2Rail, CONNECTA and the X2Rail that completed work on Train Control and Monitoring Systems (TCMS) and cyber-security through Shift2Rail.
4) **Monitoring of the latest trends:** Rail must continue to be aware of advancements in research areas such as Supercomputing, Quantum Computing, Blockchain and AI to ensure alignment and anticipation of their possible impacts on the European cyber-security system.

Challenges for the European Rail sector

➔ ***Short-term challenges with high priority (1 – 3 years)***

The Technical Specification in CENELEC TC 9X WG 26 must be completed

Short-term challenges are primarily caused by the requirement to complete legislation. The Technical Specification 50 701, under way by CENELEC/TC9X/WG26, is the most promising way to rectify short-term obstacles. Due to the time constraint and rather large number of topics addressed by CLC/TS 50 701, UNIFE believes that all stakeholders should commit considerable resources towards its completion. CLC/TS 50 701 should aim to be published by early 2021.

A clarification of the regulatory process shall be initiated

If the CLC/TS 50 701 is to be used as a basis for authorization, regulatory processes will have to be updated and harmonised. Formally, this can only be done after the CLC/TS 50 701 is completed and evolved into an EN standard. However, due to time constraints of the process, it is desirable for the update and harmonisation of regulatory processes to be prepared in parallel. Until an EN standard is available, it is the UNIFE position that a self-declaration, company certification (analogue to ISO 27001) and/or a process certification (IEC 62443-2-4 and/or -4-1) should suffice regarding cybersecurity regulation.

Convergence of CENELEC Standardisation and EU R&D&I project (e.g. Shift2Rail and its successor in Horizon Europe)

There must be a strong interaction between CENELEC and EU R&D&I projects such as Shift2Rail and Horizon2020. The results achieved by EU R&D&I projects can be used in standardisation approaches and resolved issues identified in standardisation/regulation efforts, inspiring research topics for future EU R&D&I projects. This cooperation must be reinforced in Shift2Rail's successor programme within Horizon Europe.

Establishing an Information Sharing and Analysis Centre (ISAC)

ISAC initiatives are encouraged by the Commission and ENISA. Through such institutions, a European Rail-ISAC (ER-ISAC) is established by infrastructure managers and railway undertakings from Belgium, France, Germany and the Netherlands, and is open to other European Member States. UNIFE supports the ER-ISAC's activities and is willing to maintain an open and positive dialogue to better understand how it will bring benefits to the manufacturers.

UNISIG position on Cyber Security in preparation of the next CCS TSI

Concerning the Control command and signalling (CCS) TSI, UNISIG members are actively involved in the development of the future European Rail Traffic Management System (ERTMS) game changers, in coordination with Shift2Rail Innovation Program 2 and within the European Rail Agency (ERA) coordination groups dealing with the ERTMS. The most important enablers are Automatic Train Operations (ATO), ERTMS Level 3, Future Railway Mobile Communication System (FRMCS) and Cyber Security. Concerning the latter, the main aim is to achieve the optimal level of protection against any significant threat to the signalling and telecom systems Europe relies on in the most economical way.

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

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

Ensure that the cybersecurity is appropriately addressed in new and existing TSI

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

➔ ***Mid-term challenges (4 – 6 years)***

The CLC/TS will be applied to projects

Once the CLC/TS is stable, it must be rolled out in companies. Initially, it will be implemented on a project basis, while the long-term goal is to reach a state in which processes, and not projects, 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.

The CLC/TS 50 701 is to be further developed into a CENELEC Standard (EN)

Due to the time pressure to complete the CLC/TS, it can be anticipated that not all targeted topics will be covered in depth. Further, the application of the CLC/TS to projects will lead to new insights. Hence, after applying the CLC/TS to a few projects, a further development of the CLC/TS into an EN Standard is desirable. The CLC/TS will be the base document and will be enhanced with the collected experience for such a future EN Standard for railway. Once the standard is ready, it must be decided if a certifying body is needed. In that case,

the relationship to the safety authorization process, which has moved from the national level to the European Union Agency for Railways (ERA), must be coordinated. This must be a harmonised, adequate and aligned approach that covers the different natures of safety and security.

The entire supply chain shall be secured

Together with rolling out the process as described in the CLC/TS, it is important to secure the entire supply chain. The implementation of security targets will only work if the related suppliers along the complete chain are involved and know how to create secure products and subsystems. UNIFE members can contribute to implementing security features and processes across complete rail systems. It must be noted that the supply chain also includes cloud services - on whose suppliers the railway stakeholders have very little influence.

Quantum-Security and Crypto-Agility

As quantum technology grows, 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/asymmetric cryptography which underpin the infrastructures and networks.

The European Rail Supply Industry needs to make their 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.

While such Quantum-Secure algorithms or Post-Quantum Cryptography are not yet ready for deployment and a Post-Quantum Cryptography Standardisation process from NIST is not expected before 2022-2024, industry must already start to prepare by implementing crypto-agility into devices and systems with relevant protection needs today. This will permit the ability to change parameters or schemes dynamically while maintaining the operation of protocols, applications, and processes so that these systems may be securely upgraded as the threat to today's public key cryptography becomes relevant.

Technologies to secure multi-modal and intermodal mobility are to be developed

Digitalisation is set to be a driver for multi-modal mobility, where travel by air, rail and road will be integrated. This will require an integration of the three's IT-systems, which means their respective cyber security methods must be harmonised. There is ongoing research on this topic within Shift2Rail today, which will be developed to provide for the sustainable, smart, multi-modal transport of people and goods by employing V2X and 5G communication technologies. Shift2Rail's successor within Horizon Europe should address this topic.

➔ ***Long-term challenges to be monitored for next priorities (7– 9 years)***

Processes, and not anymore projects, will be authorized

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

For next generation systems, the entire product lifecycle must be secured

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.

An international standard should be created

The CENELEC EN standard mentioned above must go to IEC with the goal to have an international standard based on it.

Key messages and Recommendations

UNIFE believes that to reach full cooperation in the European cyber-security sphere there must be a cooperative approach by all necessary stakeholders, in both standardisation and R&D&I activities. Therefore:

1) **To the European Commission (DG CONNECT)**
   UNIFE calls for a harmonisation of NIS Directive implementation in the different Member States considering consistent implementation. A balance between the level of detail of a regulatory framework and the pace of continuing IT development is to be considered before further legislative activity is desirable.

2) **To the European Commission (DG RTD, DG MOVE, DG CONNECT)**
   UNIFE also calls on the EU to allocate more funding for railway research to ensure that Shift2Rail is extended in Horizon Europe. This will address railway cyber-security priorities and continue the work started by current Shift2Rail and others European research projects.

3) **To ENISA**
   UNIFE asks ENISA to include railways in its cyber-security strategy, and to associate UNIFE to any development linked to the sector.

4) **To CENELEC/TC9X/WG26**
   UNIFE calls on Working Group 26 experts to finalize and publish the Technical Specification 50 701 to apply the IEC 62443 standard "*Security for industrial automation and control systems"* to the railway sector.

Conclusions

In this vision document, the rail sector's short-term, mid-term and long-term cyber-security challengers are outlined. For rail transport, the first step is to create a clear, strong CENELEC Technical Specification that can be used for the coming years. This is a living document which will be updated regularly according to new developments and needs that will be identified as these technologies progress.