STRATEGIC POSITION REPORT

STRANE

STRatégie d'Action de l'EPSF au Niveau Européen
(the European Strategy Action of EPSF)
in consultation with the French sector

GT2

Cybersecurity

1 ■ Introduction and background information

2 ■ Current situation and avenues for consideration

3 ■ Summary: Position of the French railway sector in response to regulatory trends in cybersecurity

STRANE: **STR**atégie d'**A**ction de l'EPSF au **N**iveau **E**uropéen (the European Strategy Action of EPSF) in consultation with the French sector

Strategic position report

GT2: Cybersecurity

Date / version: 07/11/2025 – V2.0

Organisations represented:

- AFRA
- AGIFI
- ALSTOM GROUP
- ANSSI
- CERTIFER
- EPSF
- HEXAFRET
- Lisea
- RLE
- SNCF Réseau
- SNCF SA
- SNCF Voyageurs
- UTPF

1. Introduction and background information

Cybersecurity is a growing concern in the railway sector, particularly in terms of railway safety, alongside technological developments and, more generally, digitalisation. With the aim of improving safety, competitiveness, performance and developing new services, an increasing number of systems are now interconnected and rely on the use of new technologies (cloud, AI, etc.), IT systems and networks. These changes are giving rise to new vulnerabilities that can compromise both the safety of people and property as well as the continuity of operations.

In this context, new European regulations (including the NIS2[1] Directive and the CRA[2] Regulation) are emerging and apply across the board to activities and products without necessarily taking into account the specific characteristics of the railway sector, such as the very long service life of equipment. Railway infrastructure and rolling stock incorporate technologies that are becoming obsolete at an accelerated rate due to rapid technical developments and constantly evolving cybersecurity threats. This is causing a misalignment between current regulatory compliance

[1] NIS2: DIRECTIVE (EU) 2022/2555 Network and Information Security, directive published in the Official Journal of the European Union in December 2022

[2] CRA: REGULATION (EU) 2024/2847 Cyber Resilient Act entered into force on the 10th of December 2024

Disclaimers: This document is a summary of the discussions and common positions shared by the stakeholders of the STRANE working group. The document is not intended for public dissemination and does not under any circumstances engage the responsibility of the associated entities. However, with regard to its content and the identified common positions, each participant is free to use it as they see fit for their own purposes.

assessment systems and the frequency with which mitigation measures (changes to procedures, configurations, corrective measures, etc.) need to be implemented.

The question of an effective, compatible and proportionate regulatory framework for railway sector arises. Therefore, it is essential to provide a clear vision and to establish a sustainable and realistic framework. This must include consideration of certification schemes for rolling stock and equipment (demonstration of compliance) and an optimised mechanism to report cybersecurity incidents. Furthermore, the increasingly close links between manufacturers and operators, particularly in terms of maintenance, also pose a challenge for cybersecurity throughout the value chain. Finally, the increase in the number of players as a result of the market opening up to competition is making the roles and responsibilities of Infrastructure Managers and Railway Undertakings increasingly complex, while the railway system is becoming ever more integrated (ERTMS and CBTC). The work currently underway to develop a standard dedicated to railway cybersecurity, or to be carried out in the future with the update of the Technical Specifications for Interoperability (TSIs), must move in this direction in order to contribute to an effective regulatory framework and economically sustainable.

2. Current situation and avenues for consideration

- Regulatory complexity, overall consistency and demonstration of compliance, cybersecurity scope of TSIs

At first glance, railway regulations do not appear to include cybersecurity: it is difficult to find the word cybersecurity written in full in any TSI or CSM. However, requirements may arise:

- In the CCS TSI[3], the reference to the 2018 revision of standard EN 50129[4] introduces cybersecurity factors.
- Similarly, a fairly broad interpretation of Regulation (EU) 2018/7625 could lead to an organisation's cybersecurity policy being examined in connection with the issuance of a security certificate or an approval, with the risk of introducing heterogeneous requirements.

The authorisation processes (vehicles and fixed installations) require applicants to carry out a process of gathering requirements that go beyond purely railway-related requirements. This means that applicants must certify that they have taken into account the various regulations that may apply.

Thus, cyber non-railway "cross-cutting" regulations apply to organisations: infrastructure managers, railway undertakings and their systems (in particular NIS2, REC[6], CRA and RED[7]). Where the directives are concerned, their necessary transposition into national law may introduce disparities between Member States.

How can one navigate this regulatory landscape? Railway regulations regarding cybersecurity are still very much in their infancy. Conversely, "cybersecurity" regulations propose a set of measures,

[3] Implementing Regulation 2023/1695/EU "Control-Command and Signalling"
[4] Railway applications - Communication, signalling and processing systems
[5] In accordance with directive 2016/798 and the order of 4 January 2016 on the classification nomenclature for railway safety events.
[6] Directive 2022/2557/EU on the resilience of critical entities
[7] Directive 2014/53/EU concerns the placing of radio equipment on the market

Disclaimers: This document is a summary of the discussions and common positions shared by the stakeholders of the STRANE working group. The document is not intended for public dissemination and does not under any circumstances engage the responsibility of the associated entities. However, with regard to its content and the identified common positions, each participant is free to use it as they see fit for their own purposes.

sometimes uncoordinated, that aim at increasing the level of cybersecurity applied to the railway sector. It is essential to ensure that the two approaches, railways and cybersecurity, are compatible in order to achieve a safer and more efficient system. In case of regulatory changes or conflict, the choice of measures must be based on an assessment of the specific constraints of the railway sector, taking particular account of the principles of safety or Common Safety Method, the longevity of equipment as well as issues of technical and industrial feasibility. This approach will ensure that regulations are tailored to the realities of the railway system and the industry.

Cybersecurity activities do not end once authorisation has been obtained: the evolving threat requires a risk-based approach and continuous monitoring to ensure that the measures implemented remain relevant and effective. Railway or cybersecurity regulations require incident notification and, where applicable, a report to be produced. If an incident affects both railway safety and cybersecurity, or other aspects, the operator may have to make multiple reports, which should be rationalised.

- Cyber critical assets: ensure harmlessness to speed up patches

A system considered to be cyber-secure at a given moment may become vulnerable the very next day, requiring quick patches or mitigation measures. However, these interventions must be aligned with regulatory assessment timelines, which are frequently incompatible with the urgency of updates, particularly due to the stringent assessment procedures applied to modifications affecting railway subsystems.

One possible way to avoid this pitfall is to define a list of critical components in terms of cybersecurity (Cyber Critical Assets) in advance, based on criteria to be defined. Through their design and system architecture, these components must guarantee that they do not compromise railway safety, regardless of the corrective measures applied to them (e.g. upgrading a firewall without impacting the qualification of the functional controllers that surround it). This principle is also in line with the recommendations of standards EN 50129[4] and EN 50159[8] on system architecture, which aim to separate functional safety aspects from cybersecurity aspects. The criteria used to define these critical components could be developed by industry players at the European level through a working group and in consultation with the authorities. Thus, cybersecurity patches could be rolled out by the manufacturer or operator in accordance with cross-cutting cybersecurity regulations, based on provisions defined in advance in the authorisation or certification application file.

- Clarification of responsibilities and coordination for railway cybersecurity

Changes in the regulatory environment for cybersecurity require clarification of the roles between the authorities responsible for the security of information systems (ANSSI in France) and railway safety (EPSF in France). Should the role of railway NSAs (National Safety Authorities) be expanded to include specific responsibilities in the area of cybersecurity?

[8] Railway applications - Signalling, telecommunications and processing systems - Safety-related communication in transmission systems

Disclaimers: This document is a summary of the discussions and common positions shared by the stakeholders of the STRANE working group. The document is not intended for public dissemination and does not under any circumstances engage the responsibility of the associated entities. However, with regard to its content and the identified common positions, each participant is free to use it as they see fit for their own purposes.

Furthermore, the presence of multiple players occupying various roles within the railway system highlights the need for enhanced coordination and clarification of responsibilities, particularly in order to secure interactions between entities whose cybersecurity capabilities and maturity may vary.

Finally, demonstrating compliance with the requirements of the NIS2 directive and the CRA regulation must take into account the fact that the main railway subsystems consist of an assembly of products, and result in operational implementation procedures. Consistent sector-specific regulations and a more precise definition of how these cross-cutting regulations are to be applied could address this requirement.

3. Summary: Position of the French railway sector in response to regulatory trends in cybersecurity

Against a backdrop of stricter European cybersecurity requirements, the French railway sector is adopting a strategic approach based on three fundamental principles to safeguard compliance, operational relevance and document efficiency.

1. Maintain regulatory compliance

The aim is to establish consistency between the various regulatory frameworks. The **NIS2** directive and the **Cyber Resilience Act (CRA)** complement each other in terms of cybersecurity:

- The **NIS2** is primarily aimed at **entities** and how they are **organised (operators, manufacturers, industrial stakeholders)**, with a focus on **governance**, **internal processes**, the **supply chain** and the **management of risks** related to information systems.
- In contrast, the **CRA** is aimed at product suppliers and acts as a **technical lever**, by targeting **products** and their **intrinsic security**. It demonstrates the **technical compliance** of equipment and software.

This breakdown of roles enables **cybersecurity risks to be managed more effectively**: companies can use the CRA requirements to **identify and mitigate vulnerabilities** in their products and services, thereby facilitating the achievement of NIS2 objectives, namely **protecting their networks and information systems** against cyber threats.

The TSIs[9] must be **compatible with the CRA** and even with the NIS2 directive. In order to guarantee secure interoperability across Europe, the cybersecurity requirements that may be included in future developments of TSIs must be aligned with cross-cutting cybersecurity regulations and highlight the relationship with the requirements arising from these regulations.

[9] Of which OPE TSIs (Implementing regulation 2019/773/EU "Operation and traffic management of the rail system", TAF TSI Implementing regulation 2021/541/EU **"Telematics applications for freight services"** and TAP TSI Implementing regulation 2011/454/EU "Telematics applications for passenger services" are excluded.

Disclaimers: This document is a summary of the discussions and common positions shared by the stakeholders of the STRANE working group. The document is not intended for public dissemination and does not under any circumstances engage the responsibility of the associated entities. However, with regard to its content and the identified common positions, each participant is free to use it as they see fit for their own purposes.

2. Prioritise efforts and optimise the implementation of cybersecurity measures

Faced with the complexity of systems and the diversity of assets, the sector wishes to prioritise its efforts by:

- **Focusing on CCAs (Cyber Critical Assets)**: whether they are existing (legacy) assets or critical components in recent/future projects, CCAs are central to security measures (Maintenance in Secure Condition – MCS) and must therefore be precisely identified. This notably includes the management of corrective measures, which must be carried out within the framework of the CRA to provide continuous and documented security.
- **Giving priority to COTS (Commercial Off-The-Shelf) products**: off-the-shelf products, sometimes used as CCAs, are a lever to deploy cybersecurity through a volume effect.

To avoid duplication and maximise efficiency, the sector recommends:

- **Using the railway cybersecurity standards IEC 63452** (currently under development) **and TS 50701**: these standards make it possible to produce deliverables that can be **reused directly** in CRA and NIS2 compliance procedures, thus avoiding duplication of documentation.

3. Provide effective cybersecurity coupled with control over railway safety

- **Optimise demonstration procedures**

Anticipating cybersecurity deployment conditions in the context of railway safety is a key issue that the sector must consider in order to ensure that it can respond quickly and effectively to cybersecurity issues. Clearly defined cybersecurity processing conditions and criteria (particularly around the CCA approach) in line with operational safety control requirements should enable cybersecurity patches to be deployed while limiting railway safety demonstrations and, *by extension*, obtaining new authorisation from a NSA.

- **Regulate demonstrations through a harmonised sectoral approach**

The conditions and criteria for cybersecurity deployment must be defined by operational safety and cybersecurity experts in the sector, in conjunction with the relevant safety authorities (ERA/NSA for railway safety, ENISA for cybersecurity) in order to achieve harmonised and effective application across all projects and the European railway sector supply chain.

- **Legacy equipment**

The transition of the railway sector towards more cyber-secure systems will apply principles of transition and prioritisation for legacy equipment, enabling it to remain in service while progressively moving towards compliance, in proportion to risks identified or opportunistically when a modification is implemented.

Disclaimers: This document is a summary of the discussions and common positions shared by the stakeholders of the STRANE working group. The document is not intended for public dissemination and does not under any circumstances engage the responsibility of the associated entities. However, with regard to its content and the identified common positions, each participant is free to use it as they see fit for their own purposes.

STRANE