European Strategy Action of EPSF developed in coordination with the French railway sector Cybersecurity

Denis Garnier EPSF (NSA FR)

Tallinn, 02/12/2025

Why a European Strategy Action for a NSA?

STRANE?

• **STR**atégie d'**A**ction de l'EPSF au **N**iveau **E**uropéen

(European strategy action of EPSF (NSA FR))

Context

• Part of development of EPSF (NSA FR) European strategy

• Needs commonly identified with the French sector to bring and support common positions at European level, in a moving regulatory landscape, for a better impact and efficiency

• In coordination with the French Transportation Ministry

Goals

• Identify the main strategic topics (long term and impactful)

• Act in a proactive manner regarding the evolution of regulations – not only react to and avoid being surprised

• Influence at an early stage the regulatory évolutions and lead the necessary actions at the right time and the right place (to take into account national speficities and expectations).

Organisation

Decision following 2 first STRANE plenary meetings

Creation of 3 working groups working on:

- Regulations stability
- **Cybersecurity**
- Return of experience

Organisation of cybersecurity working group

4 (remote) meetings:

- 1 meeting for open discussion
- 1 meeting for writing positions
- 2 meetings for reading and amending positions

Participants

An important variety of participants

- Railway undertakers
- Infrastructure managers
- Industry
- Evaluation bodies (such as NoBo, DeBo, Asbo)
- Associations (RU, IM, industry)
- State authorities (cybersecurity, NSA)

Various cybersecurity policies and awareness levels

- Highly staffed railway « pure players »
- Railway subsidiaries of bigger non railway organisations
- « Small » actors (represented by their association)

List of participants

- AFRA
- AGIFI
- Alstom Group
- Certifer
- Hexafret
- LISEA
- RLE
- SNCF Réseau
- SNCF SA
- EPSF
- SNCF Voyageurs
- UTPF
- ANSSI

Where we are

Regulatory aspects

- Railways regulations (TSIs, CSMs): no explicit requirement for cybersecurity but can called through a standard or a comprehensive reading of regulations (resilience)
- « Requirements capture » (PA VA) : general cybersecurity requirements + specialised regulations (radio). Risk of discrepancies in directive transpositions.
- « Lex Specialis » principle: in case of conflict, which regulation prevails?

Cybersecurity and projects lifecycle

- Need for an economically sustainable approach
- Need for a continuous monitoring, risk based approach
- Possible multiple events notifications (and, when applying, of multiple reports)
- Impact on railway safety of cybersecurity risk mitigation measures or of patches?

Summary of positions (1/2)

Nota

Following amendment requirements during STRANE plenary meeting on 26/11/2025, these positions may be subject to slight modifications (issue of legacy systems).

Ensure regulation compatibility

- NIS2 is aimed at entities (RU, IM, manufacturers) and to their organisation (processes, etc.)
- CRA is aimed at product suppliers (technical lever)

CRA may be used to demonstrate the fulfilment of NIS2 directive requirements. Need of TSI compatibility with these cybersecurity requirements.

Summary of positions (2/2)

<u>Prioritise efforts and optimise the implementation of cybersecurity measures</u>

- Concentrate on CCA (Cyber Critical Assets) which have to be identified
- Give priority to COTS (commercial off-the-shelf) for CCA
- Rely on deliverables coming from standards implantation (TS 50701 and PT 63452) to demonstrate conformity to regulation.

<u>Allow a cybersecurity coordinated with the control of railways safety</u>

- Anticipate cybersecurity issues in the context of railways safety, to limit demonstrations for a first authorization and avoid further applications for authorizations
- Conditions and criteria for cybersecurity measures to be defined commonly between railways safety authorities and cybersecurity authorities

Utilisation of positions

Stakeholders are invited to convey the recommendations of the position paper within their relevant influential bodies, particularly in the context of regulatory changes.

Thank you for your attention!

Interested to know more about the EPSF's take on railway safety and interoperability?

Check out our Vision document:

Check out our dedicated playlist: