DECISION OF THE SYSTEM PILLAR STEERING GROUP
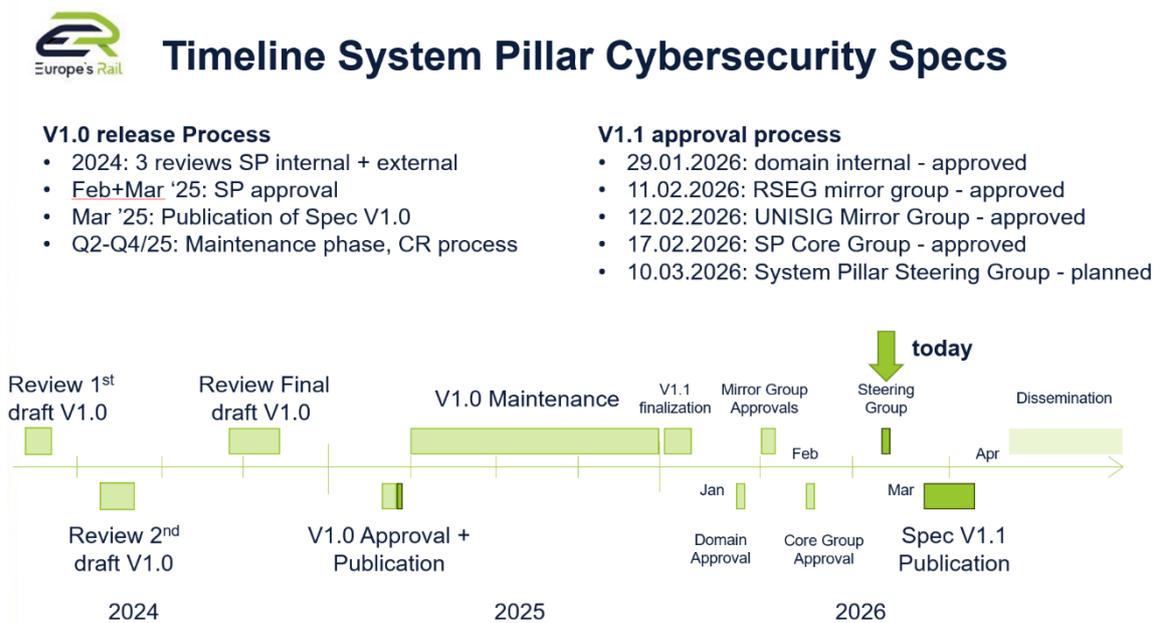
adopting the publication of the V1.1 of the System Pillar Cybersecurity specification

N° 1/2026

THE SYSTEM PILLAR STEERING GROUP OF THE EUROPE'S RAIL JOINT UNDERTAKING, NOTES

- The elements of Version 1.1 of the System Pillar Cybersecurity specifications are as follows:
  - Main specification:
    - Secure Component Specification V1.1
    - Secure Communication Specification V1.1
    - Shared Cybersecurity Services Specification V1.1
    - Secure Program Requirements V1.1
  - Supporting documentation:
    - Taxonomy & References V1.1
    - Regulatory Compliance Tracing V1.1
    - Support for essential functions V1.1
    - System Description V1.1
    - Initial Risk Assessment V1.1
    - Threat Catalogue V1.1
    - Product Documentation Template V1.1
    - Migration Guideline V1.1
    - Detailed Risk Assessment V1.1
    - Detailed Risk Matrix V1.1

- The EU-RAIL System Pillar cybersecurity specification documents provide a detailing of the requirements from regulations and standards for interoperability and for a common level of component security for rail consistent with four EU regulations and directives (NIS2, CSA, CRA, RED) and four international standards (IEC 62443-2-1, IEC 62443-4-2, CENELEC TS 50701, IEC PT 63452), with which compliance is required for rail suppliers, and operators of rail infrastructure managers and rolling stock. It is the view of the sector as expressed through the work of the SP cybersecurity domain that the additional specifications described are necessary to facilitate interoperability; reliance on the EU regulation and international standards alone is not sufficient.

- The EU-RAIL System Pillar V1.0 specifications were approved in 2025 (reference SP-STG Decision 03/2025). The content of V1.0 of the spec was finalized following a 3-round review by the System Pillar Core Group and domains, as well as a 2-round review by external entities (UNIFE, UNISIG, EIM, RSEG, ERA, ENISA).

- After the release of the V1.0 of the specifications, the documents were immediately subject to maintenance review to improve the quality of the documents. Since the release, the domain has received a number of change requests that were processed according to the SEMP change process within the group. The changes were reviewed by the mirror groups as part of the SEMP process.

- The changes between V1.1 and V1.0 are categorized as follows: 27 editorial changes, 49 text clarifications, 9 functional improvements and 18 error correcting changes based on received input after the V1.0 release.

- The approval process within the System Pillar has been followed, and the relevant approvals are granted. All changes to V1.0 that form the V1.1 were approved in consensus within the group. The cybersecurity specification has been approved by all members of the System Pillar Cybersecurity domain, and by the UNISIG Cybersecurity mirror group and EUG Rail Security Expert mirror group, summarised as follows

Timeline System Pillar Cybersecurity Specs

V1.0 release Process
- 2024: 3 reviews SP internal + external
- Feb+Mar '25: SP approval
- Mar '25: Publication of Spec V1.0
- Q2-Q4/25: Maintenance phase, CR process

V1.1 approval process
- 29.01.2026: domain internal - approved
- 11.02.2026: RSEG mirror group - approved
- 12.02.2026: UNISIG Mirror Group - approved
- 17.02.2026: SP Core Group - approved
- 10.03.2026: System Pillar Steering Group - planned

- Following approval, the documents will be made freely available on the EU-RAIL website, and contain standard title page and disclaimer of Europe's Rail System Pillar allowing free access.

- The documents for publication contain the following maintenance note:

  After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address: cybersecurity.review@ertms.be

- For information, the specifications are of potential future relevance to the Technical Specifications for Interoperability in detail:

- The technical System Pillar Cybersecurity specifications (Secure Communication Specification and Shared Cybersecurity Services Specification) are required for technical interoperability and therefore candidate to be referenced for security update of TSIs.
- The Secure Component Specification defines a common level of component security with no interoperability requirements. It is therefore not planned to be referenced in TSIs, though it is still important to ensure an appropriate cybersecurity level.
- The Secure Program Requirements define cybersecurity requirements for processes of operators (and suppliers). This requirement specification is planned for TSI application guidance since it provides structured implementation instructions based on international standards, allowing traceable compliance with EU regulation (e.g. NIS2) in day-to-day operations.

- The specifications support the development and harmonisation of Shared Cybersecurity Services, which ease the development of cybersecure components by defining Europe-wide standard interfaces e.g. for certificate management, security logging, single sign-on.

- The EU-RAIL System Pillar Cybersecurity specifications are also relevant to the outputs of other specification development work – for example System Pillar domains, the Innovation Pillar (DAC, Digital Map,…), UIC (FRMCS), EGNOS,… to close the gap for cybersecurity regulation and standards compliance.

THE SYSTEM PILLAR STEERING GROUP OF THE EUROPE'S RAIL JOINT UNDERTAKING, AGREES

- To publish on the EU-RAIL website the EU-RAIL System Pillar Cybersecurity specification V1.1 (four main specifications and ten supporting documents).

ANNEX

- See associated document set "System Pillar Cybersecurity specification V1.1"