

DECISION OF THE SYSTEM PILLAR STEERING GROUP

adopting the publication of the System Pillar Cybersecurity specification

N° 3/2025

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

- The cybersecurity specification within rail, provides
 - Compliance 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) is required for rail suppliers, and operators of rail infrastructure managers and rolling stock.
 - Details the requirements from regulations and standards for interoperability and for a common level of component security.
 - The technical System Pillar Cybersecurity specification (Secure Communication Specification and Shared Cybersecurity Services Specification) are required for technical interoperability and therefore planned for security update of ERA TSIs.
 - The Secure Component Specification defines a common level of component security with no interoperability requirements
 - The Secure Program Requirements define cybersecurity requirements for processes of operators (and suppliers). This requirement specification is planned for TSI application guidance since implementation is required for compliance with EU regulation.
 - The Cybersecurity specification shall also supports other System Pillar domains, the Innovation Pillar (DAC, Digital Map,...), UIC (FRMCS), EGNOS,... to close the gap for cybersecurity regulation and standards compliance.
 - Support to the development and harmonisation of Shared Cybersecurity Services, which ease the development of cybersecure components by defining Europe-wide standard interfaces for certificate management, security logging, single sign-on,...
- The Cybersecurity specification has been created by analyzing 42 existing cybersecurity documents specific to the railway sector as well as relevant EU cybersecurity regulations and international cybersecurity standards.
- The deliverables will be made public to every stakeholder.

- The approval process within the System Pillar has been followed, and the relevant approvals are granted.
- Particularly, the Cybersecurity specification has been approved by all 18 members of the System Pillar Cybersecurity domain, and by the UNISIG Cybersecurity mirror group and EUG Rail Security Expert mirror group.
- The content defined in this release 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)



- The documents for publication contain the following disclaimer allowing free access:

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains.

EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used. EU Rail authorizes you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following mention [EU Rail trade mark, title of the document, year of publication, version of document, URL].

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trademarks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.

EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

- 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

- The elements of Version 1 of the System Pillar Cybersecurity specifications are as follows:
 - Main specification:
 - Secure Component Specification V1.0
 - Secure Communication Specification V1.0
 - Shared Cybersecurity Services Specification V1.0
 - Secure Program Requirements V1.0
 - Supporting documentation:
 - Taxonomy & References V1.0
 - Regulatory Compliance Tracing V1.0
 - Support for essential functions V1.0
 - System Description V1.0
 - Initial Risk Assessment V1.0
 - Threat Catalog V1.0
 - Product Documentation Template V1.0

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

- To publish as System Pillar documents on the EU-RAIL website the EU-RAIL System Pillar Cybersecurity specification V1.0 (four main specifications and seven supporting documents).
- To publish an update, once the training material is complete in the ERA github/gitlab for additional information.

ANNEX

- See associated document set “System Pillar Cybersecurity specification V1.0”