Release Note - Cybersecurity Specification V1.0

1 Preamble

1.1 Change history

Version	Release date	Modified sections
V1.0	2025-02-20	All sections - first version

1.2 Confidentiality classification

Public

1.3 Purpose of the release

This release is foreseen for publication as output of System Pillar (System Pillar website).

The type of baseline is (according to Configuration Management Plan):

Purpose of release	
System Pillar Document Release	X

1.4 Scope of this document

This Release Notes describes an (internal or external) delivery from **System Pillar**. The System Pillar is the “generic system integrator” for the Europe’s Rail Joint Undertaking (**EU-Rail**), and the architect of the future EU’s railway system. For more information, see ERJU System Pillar website

This release includes several new documents. Content which belongs to the specification in strict sense is being prepared in a systematic engineering approach.

1.5 Restrictions of use

The Cybersecurity specification have following restrictions:

- Compliance tracing to IEC PT 63452 uses a intermediate draft version from Jan 2025. The final standard is expected later in 2025. The Cybersecurity specification will be updated once the standard is finalized
- For EU CRA regulation harmonized standards are being developed. Once draft and final version will be availble, an update of the Cyberseucrity specification is forseen.
- Cybersecurity certification aspects and EU CE conformity requirements are not included in this version of the specifications. This aspects will be investigated in future work of the Cybersecurity domain.

1.6 Configuration database (mandatory)

The Cybersecurity specification delivery documents are located in Polarion (SP-PRAMSS - 62 Security - 20 Deliverables)

Polarion SP-PRAMS - SP Cybersecurity Domain - Deliverables

1.7 Legal information and feedbacks

The release is delivered under the above copyright information.

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

2 Release content

This section gives the list of main configuration items delivered with their version.

2.1 Documents addressed by the release

The documents covered by this release are:

Capability name	Change (new|modified|unchanged)	Comment
Secure Component Specification	new	V1.0
Secure Communication Specification	new	V1.0
Shared Cybersecurity Specification	new	V1.0
Secure Program Requirements	new	V1.0
Regulatory Compliance Tracing	new	V1.0
System Description	new	V1.0
Support for essential functions	new	V1.0
Initial Risk assessment	new	V1.0
Threat catalog	new	V1.0
Product Documentation Template	new	V1.0
Taxonomy & References	new	V1.0

2.2 Main enhancements from the previous release

No previous release.

2.2.1 Secure Component Specification

The Secure Component Specification is a Cybersecurity Requirements Specification (CRS) according to IEC 62443-3-2, CENELEC-CEN TS 50701 and IEC PT 63452.

2.2.2 Secure Communication Specification

To provide cybersecure interoperable data transmission the Secure Communication Specification defines technical requirements based on the ETCS end-to-end security layer (see subset 146) and EULYNX BL 4.0.

2.2.3 Shared Cybersecurity Services Specification

A cybersecure state within a “secure component” can only be guaranteed via integration with central cybersecurity services. The Shared Cybersecurity Services Specification provides requirements for these services and their interfaces.

2.2.4 Secure Program Requirement Specification

On the structural basis of 62443-2-1, which was updated in 2024, the Secure Program Requirement document combines the necessary processes and specifications.

2.2.5 Supporting documents

The seven supporting documents permit additional application cases of the four main specifications.

2.3 Configuration items

2.3.1 Documents configuration

Document iD	Document Name	Name of Document Baseline in Polarion
10 SP-SEC-Tax	10 Taxonomy and References	V1.0 first release
20 SP-SEC-Comp	20 Secure Component Specification	V1.0 first release
21 SP-SEC-Comm	21 Secure Communication Specification	V1.0 first release
22 SP-SEC-Serv	22 Shared Cybersecurity Services Specification	V1.0 first release
23 SP-SEC-Pgrm	23 Security Program Requirements	V1.0 first release
30 SP-SEC-RegCompl	30 Regulatory Compliance	V1.0 first release
31 SP-SEC-DocTempl	31 Product Documentation Template	V1.0 first release
32 SP-SEC-EssFunc	32 Support for Essential Functions	V1.0 first release
40 SP-SEC-IRA	40 Initial Risk Assessment	V1.0 first release
41 SP-SEC-ThreatCat	41 Threat Catalogue	V1.0 first release
42 SP-SEC-SysDesc	42 System Description	V1.0 first release

2.4 More information

Maintenance

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

3 Problems Fixed (mandatory)

First release. No previous change request exisiting.

Change Request Id	Change Request Type	Change Request title	SP Domain/task who has managed the Change Request

4 Known open problems, issues

Note to author: This paragraph shall address the main issues known and not yet fixed in the release, sorted by severity.

CR or Issue Id	Issue Severity	Change Request or Issue title	Scheduled release for correction	Comment
SPPRAMSS-13988	Low	Avoid duplicate certification	Jan 2026	Certification discussion planned for 2025 in SP Cybersecurity domain
SPPRAMSS-13987	Low	Align with upcoming CRA horizontal standard	Jan 2026	waiting for draft of horizontal standard (April / Mai 2025)

5 APPENDIXes

5.1 Release Note Verification and Configuration Review (mandatory - by Quality Manager)

This appendix shall address the validation of the Release Note by **Quality Manager** and the conformity of the Release Note to the Configuration managed in the Configuration Management Tool. This table shall be filled before sending the Release Note for review.

Num	Requirements to meet	Status OK/NOK	Comment / Action #
1	**Release Note checks**		
	The Release Note is compliant with its template. All "N/A" are justified	OK	
	The Release Note appendices are available	OK	
	The Release Note provides the usage of the delivery and its usage restrictions considering not implemented Issues	OK	
	The Release Note mentions where to find Configuration Items (Configuration Management Tools, Configuration identification)	OK	
	The Release Note associated documentation is consistent with the baseline	OK	
	In agreement with last CCB performed, the Release Note lists : - The implemented Change Requests - The corrected CRs / MRs Defect from Change Management Tool	OK	
	The Release Note lists the not implemented CRs and issues	OK	
2	**Configuration Review**		
	All the documents mentioned in the Release Note are available in configuration management tool and frozen. If not, does the release note mention derogation(s) and reason why.	OK	
	Capella mode mentioned in the Release Note is available in configuration management tool and frozen. If not, does the release note mention derogation(s) and reason why.	N/A	Capella modelling not applicable for Cybersecurity

5.2 List of Change Requests

CR list in Polarion (see also chapter 4): Change Requests

5.3 List of known issues

No known issues in this release. Issues will be tracked by CRs.