Disclaimer

This document is

the final draft created in September 2024 for the third and final review period (September 23rd - October 31st 2024) before planned publication in January 2025.

Please consider the semantics of the following **work item types** used in this document when preparing your review.

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 inthis 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.

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

SP-SEC-DocTempl-0-1, 🗎 - Regulatory compliance

This document is a template for product information required by EU Cyber Resilience Act, IEC 62443-4-1 (SG-1 to SG-8), IEC 62443 2-4, EN TS 50701 and IEC PT 63452.

[SPPRAMSS-14114 **]**

SP-SEC-DocTempl-0-2, 🗎 - Required language of technical documentation

As per EU Cyber Resilience Act, the Secure Component Documentation needs to be written in an official language of EU member states in a clear, understandable, intelligible and legible manner. **[**SPPRAMSS-14115 **]**

Work Item Type	Icon	Rationale
Text	🗎	Used for prose text, e.g. as an introduction or for additional information. The contents of these work items are **not requirements.**
Issue	☷	Used for open issues to be addressed in the final version. The contents of these work items are **not requirements.**

This document is a template for product information required by EU Cyber Resilience Act, IEC 62443-4-1 (SG-1 to SG-8), IEC 62443 2-4, EN TS 50701 and IEC PT 63452.

As per EU Cyber Resilience Act, the Secure Component Documentation needs to be written in an official language of EU member states in a clear, understandable, intelligible and legible manner.

☷**, SP-SEC-DocTempl-1 -** Analyse if this documentation information can be retrieved from the secure component **[**SPPRAMSS-10308 **]**

🗎**, SP-SEC-DocTempl-1-1,** 🗎 **- Product Name**

<Product Name> **[**SPPRAMSS-10260 **]**

🗎**, SP-SEC-DocTempl-1-2,** 🗎 **- Product Type**

<Product Type> **[**SPPRAMSS-10259 **]**

🗎**, SP-SEC-DocTempl-1-3,** 🗎 **- Product Version**

<Product Version> **[**SPPRAMSS-10261 **]**

🗎**, SP-SEC-DocTempl-1-4,** 🗎 **- Product Identification**

<serial number or batch number> **[**SPPRAMSS-10258 **]**

🗎**, SP-SEC-DocTempl-1-5,** 🗎 **- How to identify the product**

<description of how the product can be identified, e.g. locations of identifiers on labels on the product and via querying the diagnostic interface> **[**SPPRAMSS-10250 **]**

🗎**, SP-SEC-DocTempl-1-6,** 🗎 **- EU declaration of conformity**

<web address to EU declarion declaration of confirmity conformity for this product> **[**SPPRAMSS-10270 **]**

🗎**, SP-SEC-DocTempl-1-7,** 🗎 **- Software Bill of Material:**

<if made available, web address of software bill of material in CycloneDX SBOM standard format of this product> **[**SPPRAMSS-10284 **]**

, SP-SEC-DocTempl-2-1, - Manufacturer name

<Manufacturer name> **[**SPPRAMSS-10256 **]**

, SP-SEC-DocTempl-2-2, - Registered trade name or trade marktrademark

<Registered trade name or trade mark> **[**SPPRAMSS-10254 **]**

, SP-SEC-DocTempl-2-3, - Postal address

<Postal address> **[**SPPRAMSS-10255 **]**

, SP-SEC-DocTempl-2-4, - Electronic contact address

<email address or other digital contact> **[**SPPRAMSS-10251 **]**

, SP-SEC-DocTempl-2-5, - Website

<address to manufacturers contact page> **[**SPPRAMSS-10252 **]**

, SP-SEC-DocTempl-3-1, - Vulnerability information

<contact point / web site> **[**SPPRAMSS-10247 **]**

, SP-SEC-DocTempl-3-2, - Vulnerability reporting

<contact point / web site> **[**SPPRAMSS-10253 **]**

, SP-SEC-DocTempl-3-3, - Vulnerability reporting policy

<web site> **[**SPPRAMSS-10249 **]**

, SP-SEC-DocTempl-3-4, - Vulnerability handling and security update end-date

<end-date (month and year) for vulnerability handling and security update support, must be . The end-date should be the expected use-time, at least 5 years when use time is 5 years or more, or the use time if less the use time five years unless the expected use-time is less than 5 five years> **[**SPPRAMSS-10273 **]**

, SP-SEC-DocTempl-4-1, - Indented Intended purpose of the product

<description of main features and indented intended usage> **[**SPPRAMSS-10266 **]**

, SP-SEC-DocTempl-4-2, - Essential functions of the product

<description of the implemented essential functions and supported essential functions> **[**SPPRAMSS-10264 **]**

, SP-SEC-DocTempl-5-1, - Security standards compliance

<degree of compliance to referred security standards> **[**SPPRAMSS-10265 **]**

, SP-SEC-DocTempl-5-2, - Security certifications

<list of security certifications obtained for the product, link to IEC 63452 CA-01-05> **[**SPPRAMSS-10299 **]**

, SP-SEC-DocTempl-5-3, - Secure development process certification:

<list of certifications of the software development process which was applied for the development of this product, link to IEC 63452 CA-01-05> **[**SPPRAMSS-10298 **]**

, SP-SEC-DocTempl-5-4, - Defense in depth strategy

<description of the security defense of depth strategy supporting installation, operation and

maintenance> **[**SPPRAMSS-10288 **]**

, SP-SEC-DocTempl-5-5, - Security properties

<description of the security features and capabilities and their support for defense of depth strategy> **[**SPPRAMSS-10287 **]**

, SP-SEC-DocTempl-5-6, - Adressed Addressed threats

<list of threats addressed by the defense in depth strategy> **[**SPPRAMSS-10286 **]**

, SP-SEC-DocTempl-5-7, - Physical interfaces

<documented physical interfaces using photos, schematics and/or wiring schematics> **[**SPPRAMSS-10424 **]**

, SP-SEC-DocTempl-5-8, - Logical interfaces

<description of all logical interfaces / communication matrix (protocols, port numbers used, physical port used, type of data transmitted, interfacing partners)> **[**SPPRAMSS-10422 **]**

, SP-SEC-DocTempl-5-9, - Secure Component environment

<typical network architecture diagram and/or system architecture diagrams depicted the Secure Component in the system context> **[**SPPRAMSS-10423 **]**

, SP-SEC-DocTempl-5-10, - Provided security environment

<description of the provided security environment> **[**SPPRAMSS-10267 **]**

, SP-SEC-DocTempl-5-11, - Expected security environment / Security related application conditions

<list of application conditions/requirements or measures required for the integration of the product with other products or into a system and to comply with the defined security standards>standards, including physical security requirements> **[**SPPRAMSS-10283 **]**

, SP-SEC-DocTempl-5-12, - Security risks

<description of use cases which may lead to significant security risks, incl. forseeable foreseeable misuse, known product vulnerabilities and risks associated with legacy code, together with mitigation strategies to address these risks> **[**SPPRAMSS-10269 **]**

, SP-SEC-DocTempl-5-13, - Technical Security support

<description which type of security support is offered for this product> **[**SPPRAMSS-10274 **]**

, SP-SEC-DocTempl-5-14, - Changes affecting security

<description which changes can affect the security of the products> **[**SPPRAMSS-10278 **]**

, SP-SEC-DocTempl-5-15, - Tamper detection:

<documentation showing the difference between an intact and broken security seal on the product> **[**SPPRAMSS-10285 **]**

SP-SEC-DocTempl-5-16, - Physical I/O states

<documentation of the predetermined state for Secure Component with physical I/O (e.g. the safe state or degraded state)>.

[SPPRAMSS-12107 **]**

, SP-SEC-DocTempl-6-1, - Applied hardening guidelines

<list of applied hardening measures by the manufacturer or reference to applied hardening standard> **[**SPPRAMSS-10300 **]**

This following documentation topic is only relevant for components/products which are integrated with external systems (e.g. software-based products installed on a customer server or shared computing environment/cloud), integration with customers application using APIs).

, SP-SEC-DocTempl-6-2, - Additional hardening guidelines

<description of the measures for product hardening, including integration of the product in its security context, integration with customer applications, how to apply and maintain the products defense in depth strategy, how to use security options and configuration during integration> **[**SPPRAMSS-10289 **]**

, SP-SEC-DocTempl-7-1, - Initial commissioning steps

<detailed instruction on necessary measures during initial commissioning to ensure the secure use of the product> **[**SPPRAMSS-10272 **]**

, SP-SEC-DocTempl-7-2, - Security configuration options

<description of the security configuration options, their contribution to the security defense in depth strategy of the product, the default values, the configurable values and their affects effects on security, how to set, change and delete the configuration value> **[**SPPRAMSS-10291 **]**

, SP-SEC-DocTempl-7-3, - Product security permissions

<list of security permissions used for access control with their associated privileges / rights> **[**SPPRAMSS-10297 **]**

, SP-SEC-DocTempl-7-4, - Product default user accounts:

<list of default accounts used by the products and instruction how to change the account name and their credentials> **[**SPPRAMSS-10296 **]**

, SP-SEC-DocTempl-8-1, - Operational security tasks

<description of actions and responsibilities for user, including administrators> **[**SPPRAMSS-10293 **]**

, SP-SEC-DocTempl-8-2, - Operational assumptions

<description on assumptions on users behaviour related to secure operation of the product> **[**SPPRAMSS-10294 **]**

, SP-SEC-DocTempl-9-1, - Maintenance activities

<detailed maintenance instructions on necessary measures during the lifetime of the product to ensure its secure use including the periodicity of each measure/maintenance tasks, including backup and restore procedures, verification of successful backup, backup and restore related audit logs and restoration steps supporting disaster recovery> **[**SPPRAMSS-10277 **]**

, SP-SEC-DocTempl-9-2, - Additional security best-practices

<description of security best-practices for maintenance and administration of the products, as well as instructions for all recommended security-related tools and utilities that support administration, monitoring, incident handling and evaluation of the security status of the product> **[**SPPRAMSS-10292 **]**

, SP-SEC-DocTempl-9-3, - Installing security updates

<description how to verify authenticity and integrity of updates and how to install updates, including if a restart of the

product is required> **[**SPPRAMSS-10279 **]**

, SP-SEC-DocTempl-9-4, - Disable automatic security update

<description how automatic security update function is disabled> **[**SPPRAMSS-10282 **]**

, SP-SEC-DocTempl-10-1, - Decommissioning steps

<detailed instructions describing how to securely decommission the product, including how to remove the product or its intended environment, how user data, configuration data and references can be securely removed from the product and the environment, and how the product can securely disposed when not all confidential data can be removed from the device> **[**SPPRAMSS-10281 **]**