Security Program Requirements

Disclaimer

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 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

1 Table of Contents

2 Preamble

2.1 Scope, Purpose and Intended Audience

, SP-SEC-Pgrm-2.1-1 - The document provides requirements for railways (Infrastructure managers, undertakings and vehicle owners) and Suppliers to support the technical implementation and life-cycle management of Security for the system under consideration defined in Security Architecture (SuC).

, SP-SEC-Pgrm-2.1-2 - Every requirement applies for infrastructure and vehicles except a specific system or component is mentioned.

, SP-SEC-Pgrm-2.1-3 - The document provides guidance for required decisions to be taken by the railways prior to specification, tender or implementation process.

2.2 Document Usage

, SP-SEC-Pgrm-2.2-1 - This specification uses identifiers starting with "SP-SEC-Pgrm".

, SP-SEC-Pgrm-2.2-2 - Icon types used in this document are defined in SP-SEC-Tax.

2.3 References

, SP-SEC-Pgrm-2.3-1 - This chapter contains all references of this document. For a complete list including external references see [SP-SEC-Tax] Chapter 3.

[IEC 62443-2-1:2024]
Security program requirements for IACS asset owners

[IEC 62443-2-4:2023]
Security program requirements for IACS service providers

[IEC 62443-4-1:2018]
Secure product development lifecycle requirements

[ISO/IEC 27001:2022]
Information security, cybersecurity and privacy protection - Information security management systems - Requirements

[ISO/IEC 27002:2022]
Information security, cybersecurity and privacy protection - Information security controls

[NIS2 Directive]
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)

[Cyber Resilience Act (CRA)]
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)

[Cyber Security Act (CSA)]
Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

[MinElements_SBOM]
The Minimum Elements for an SBOM
https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[ERORAT Template]
EUG Risk Assessment Tool Excel based, aligned in EULYNX, EUG, RCA and OCORA.

[23E176: Procurement Guideline]
The purpose of this document is to define a guideline for the tender process to ensure similar approach, requirements, and solutions in Europe. These requirements may be used in every tender process or contract to allow similarity in service and quality.

[23E177: Security Logging Guideline]
The purpose of this document is to give guidance on architectural aspects of log data and SIEM infrastructures. Furthermore, corresponding processes are defined and explained.

[23E245: Security Penetration Testing]
The purpose of this document is to give guidance on penetration testing in the railway CCS domain (including EULYNX, ERTMS and the corresponding legacy systems).

[EUG Security Guideline]
The main objective of this document is the creation and presentation of Security Risk Assessment for System
Design process. This process is a harmonized and consolidated approach. This guideline was created in
collaboration with EUG, RCA, EULYNX and OCORA.

[SP-SEC-CompSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.0

[SP-SEC-CommSpec]

Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.0

[SP-SEC-ServSpec]

Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.0

[SP-SEC-PrgmReq]

Europe's Rail System Pillar Cybersecurity Domain - Secure Program Requirements, v1.0

2.4 Terms and Definitions

The term "supplier" is used in this document for product suppliers and integration service providers according to IEC 62443-2-4.

The term "railway" is the common definition of Infra managers, undertakings and vehicle owners in this document.

The term "railway" refers to the definition of the "asset owner" of IEC 62443-2-1.

SecRACs = Security Related Application Conditions. These application conditions need to be fulfilled to fulfill the approved level of security. SecRACs are defined in TS 50701 (draft: IEC 63452).

Dual control = Control that requires the approval by two authorised individuals in order to be performed.

2.5 Document Handling

, SP-SEC-Pgrm-2.5-1 - The requirements are structured based on the structure from IEC 62443-2-1.

, SP-SEC-Pgrm-2.5-2 - The Secure Program Spec does relate to every requirement of the IEC 62443-2-1. If not additional requirements are necessary, the original requirement of IEC 62443-2-1 is referenced to allow tracing and compliance.

, SP-SEC-Pgrm-2.5-3 - The structure is applied on the level of the main chapters per topic.

, SP-SEC-Pgrm-2.5-4 - As additional requirements have been added to support the technical specification, additional requirements that do not directly refer to an IEC 62443-2-1 requirement are available.

, SP-SEC-Pgrm-2.5-5 - As the suppliers also have to fulfill procedural requirements to support the railway's processes, a separate chapter for suppliers has been created (Chapter 14, this document).

2.6 Modification History

First release (V1.0) - February 2025

- reviewed by System Pillar domains, rail cybersecurity mirror groups, external organizations in three review rounds during 2024

3 Intentionally left blank

4 Intentionally left blank

5 Organizational Security Measures

, SP-SEC-Pgrm-5-1 - The railways shall implement an ISMS based on ISO 27001, chapter 4.4.

, SP-SEC-Pgrm-5-2 - The railway shall ensure that the railway management bodies approve the cybersecurity risk-management measures.

, SP-SEC-Pgrm-5-3 - The railway shall perform personnel background security checks for personnel which has access to to any part of the system under consideration defined in Security Architecture in the whole life-cycle (from development to decommissioning) based on ISO 27002 chapter 6.1.

, SP-SEC-Pgrm-5-4 - If suppliers have access to any part of the system under consideration defined in Security Architecture in the whole life-cycle (from development to decommissioning), the railway shall require personnel background security checks for this personnel, performed by the supplier, based on ISO 27002 chapter 6.1.

, SP-SEC-Pgrm-5-5 - If service providers have access to any part of the system under consideration defined in Security Architecture in the whole life-cycle (from development to decommissioning), the railway shall require personnel background security checks for this personnel, performed by the provider based on ISO 27002 chapter 6.1.

, SP-SEC-Pgrm-5-6 - The railway shall define a single point of contact for the exchange of security related information with suppliers.
Note: The single point of contact may be distributed to more than one person depending on technology. In case a Security Operations Center is available, the 24/7 availability could be used to allow immediate information and reaction.

, SP-SEC-Pgrm-5-7 - The railway shall define roles and responsibilities based on ISO 27002, chapter 5.2.

, SP-SEC-Pgrm-5-8 - Authorisation and authentication must be ensured before any exchange of information. The railway shall implement an appropriate method to be agreed in advance by all the contracting parties involved.

, SP-SEC-Pgrm-5-9 - Authorisation and authentication is required to ensure that the person calling or acting at the site is the person who was background checked before.

, SP-SEC-Pgrm-5-10 - The railway shall establish a security awareness and training program based on ISO 27002 chapter 6.3.

, SP-SEC-Pgrm-5-11 - The railway shall establish security responsibilities training according to IEC 62443-2-1 Org 1.5.

, SP-SEC-Pgrm-5-12 - The railway shall have policies and procedures for the management of risks based on ISO 27001 6.1.

, SP-SEC-Pgrm-5-13 - The railway shall implement processes for discovery of security

anomalies and network security based on ISO 27002 8.16 and 8.20

, SP-SEC-Pgrm-5-14 - The railway shall check the integrity of the Secure Component visually at a regular basis during maintenance.
Note: The visual integrity checks include for example the check of the tamper-evident seal, check of other damages or modifications. For this purpose a reference picture of the device and its installation place are a precondition.

, SP-SEC-Pgrm-5-15 - The railway shall define procedures to check the system integrity.

, SP-SEC-Pgrm-5-16 - The railway shall check the system integrity after an interruption of the secure component's security monitoring.

, SP-SEC-Pgrm-5-17 - If the monitoring of the secure component is interrupted, an undetected compromise could be performed. To identify this compromise, and "indicator of compromise" is needed. A process to identify this indicator of compromise is needed. This might be a visual check of the tamper-evident seal and the component itself as well as an evaluation of video surveillance material, if available.

, SP-SEC-Pgrm-5-18 - The railway shall implement secure development based on ISO 27002 8.25 for own developments and support.

, SP-SEC-Pgrm-5-19 - The railway shall require the implementation of secure development based on ISO 27002 8.25 for outsourced development and support.

, SP-SEC-Pgrm-5-20 - The railway shall implement and regular as well as event-related review its security policies based on ISO 27002 5.1.

, SP-SEC-Pgrm-5-21 - The railway shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10.

5.1 Supply Chain

, SP-SEC-Pgrm-5.1-1 - The railway shall implement supply chain security management based on ISO 27002 5.21.

, SP-SEC-Pgrm-5.1-2 - The railway shall apply the document "Procurement Guideline" from the EUG (document number: 23E176, version 1A) for Procurement Requirement specification.

, SP-SEC-Pgrm-5.1-3 - The railway shall include security requirements in the supplier qualification process based on ISO 27002 chapter 5.19.

, SP-SEC-Pgrm-5.1-4 - The railway shall ensure that requirements related to the management of service providers are implemented by the supply chain.

, SP-SEC-Pgrm-5.1-5 - The railway shall define requirements for the availability of spare parts considering security related disturbances in the supply chain.

, SP-SEC-Pgrm-5.1-6 - The availability requirements should, amongst others, also include a con tract agreements with supplier to keep and maintain a certain stock to support the disaster recovery plan.

Hint: A certain number of secure components in stock may support step by step recovery after Ransomware-attack. The plan should also reflect taken security measures to avoid spreading Ransomware (segmentation, ...) to limit the amount of stock spare parts.

, SP-SEC-Pgrm-5.1-7 - The railway shall perform a resilience analysis for services provided by service providers. [NIS 2 directive sections (85), (55), (63)]

, SP-SEC-Pgrm-5.1-8 - The railway shall perform a resilience analysis for services provided by internal service providers, e.g. the communication network service. [NIS 2 directive sections (85), (55), (63)]

, SP-SEC-Pgrm-5.1-9 - Fault tolerance of the network should be multi-fault-tolerant to be resilient against multi cause failures which is likely in big networks.

, SP-SEC-Pgrm-5.1-10 - For the resilience analysis the following services can be used as examples. The list is not complete but shall give some hints, what may be considered.
- Vulnerability Management
- Mobile Network, e.g. FRMCS, 4G, 5G
- Human Resource Management of Knowledge and Availability of work force
- Shared CyberSecurity Services, e.g. PKI service or IAM, provided by internal or external service providers

Different scenarios should be taken into consideration to perform the resilience analysis per service. Following some example scenarios are given:
- Lack of knowledge or work force due to quitting or sickness
- The service provider gets bankrupt
- The service provider is victim of a cyber security attack
- The service provider has technical problems causing unavailability including natural disasters
- The service has an (in reasonable time) unsolvable critical vulnerability

In addition it is recommended to check or let check the service providers sub-suppliers if they have relevant impact to the services for the railway.

, SP-SEC-Pgrm-5.1-11 - The railway shall implement appropriate measures according to the resilience analysis for the services which are provided by any service provider based on ISO 27002 5.21.

, SP-SEC-Pgrm-5.1-12 - The railway shall set up contractual agreements regarding availability of spare parts.

, SP-SEC-Pgrm-5.1-13 - The railway shall check periodically the effectiveness of the implemented measures regarding the resilience towards service providers based on ISO 27002 5.21.

, SP-SEC-Pgrm-5.1-14 - For a resilient rail system three main areas are relevant. First, the system architecture as it allows redundancy and even independency from specific components by design. Second, the own procedural capabilities like availability of well trained personnel, incident

management handling, etc.. Third, third party supportive services, e.g. threat hunting, 3rd level support, etc. All three elements need sufficient analysis concerning potential bottle necks that may harm the whole system operation if not available. That is why also the services provided by a service provider need to be analysed concerning the level of required resilience and according measures have to be applied.

, SP-SEC-Pgrm-5.1-15 - The railway shall check the tamper-evident seal of the transport container on arrival based on ISO 27002 chapter 5.21(j).

, SP-SEC-Pgrm-5.1-16 - The railway shall check the integrity of the Secure Component visually during hand-over phase.
Note: The visual integrity check shall uncover any modifications or damages on the secure component that may be a sign that it was compromised.

, SP-SEC-Pgrm-5.1-17 - The railway shall ensure that the tamper-evident seal of the component is checked prior to commissioning.

, SP-SEC-Pgrm-5.1-18 - The railway shall store the components in a surveyed storage with limited access with identity and access management using personal identification based on physical security in ISO 27002 chapter 7.

, SP-SEC-Pgrm-5.1-19 - The railway shall implement a multi-vendor strategy that reduces the dependency of single vendor sources based on ISO 27002 chapter 5.19 (h)-(j).

, SP-SEC-Pgrm-5.1-20 - Typical multi vendor strategies are:
- Use different network devices for redundancy in the system to avoid single source vulnerability affects.
- Maintain different vendors for security monitoring devices.
- Maintain different vendors and plan their distribution for safety related equipment to avoid single source vulnerability affects to the full network.

, SP-SEC-Pgrm-5.1-21 - The railway shall implement a strategy for purchasing technically dissimilar secure components. based on ISO 27002 chapter 5.19 (h)-(j).
Note: Technically dissimilar components shall ensure that a replacement by differently designed systems may be possible in case of major vulnerabilities. If the components are identical in their solution approach or the components used, a vulnerability may harm the overall operation, without the possibility of mitigation. Nevertheless the functionality has of course to be the same and fulfill all the functional and non functional requirements based on the available sets of requirements.

, SP-SEC-Pgrm-5.1-22 - The railway shall establish processes to reduce the dependency on suppliers of sub-components based on ISO 27002 chapter 5.19 (h)-(j).

, SP-SEC-Pgrm-5.1-23 - The railway shall audit that suppliers implement the requirements for the management of service providers based on ISO 27002 chapter 5.20 (p) and chapter 5.21.

, SP-SEC-Pgrm-5.1-24 - The railway shall set up contractual agreements regarding audit right for service providers and suppliers based on ISO 27002 5.20(p).
Note: Suppliers to railways use service providers themselves for specific needs, e.g. threat hunting, IDS capabilities, 3rd level

support, ... To ensure that these services provided by sub suppliers fulfill the same level of quality (where needed) like the suppliers, the suppliers have to implement appropriate means. The railway shall check if these means are implemented. This check should be performed through audits.

5.2 Physical Access Control

, SP-SEC-Pgrm-5.2-1 - The railway shall define processes and procedures for physical access control based on ISO 27002 chapter 7 (Physical controls).

, SP-SEC-Pgrm-5.2-2 - If any device (including cable, connector, network devices, etc.) is used to transmit data and is not protected according to requirements for protection of confidentiality or integrity of data in transit, then the railway shall realize a physical protection for the cable to mitigate residual risk based on ISO 27002, chapter 7.12.

, SP-SEC-Pgrm-5.2-3 - The railway shall define physical anti theft protection requirements for the secure component based on ISO 27002 chapter 7.8 and 7.9.

, SP-SEC-Pgrm-5.2-4 - The railway shall define physical anti theft protection requirements for the decentralized network components based on ISO 27002, chapter 7.8 and 7.9.

, SP-SEC-Pgrm-5.2-5 - The technical environment physically protecting the component shall be designed according to the local environmental threats based on ISO 27002, chapter 7.5.

, SP-SEC-Pgrm-5.2-6 - For infrastructure, the railway shall choose the location of secure components considering risk of natural disasters.

, SP-SEC-Pgrm-5.2-7 - For infrastructure, the railway shall choose the location of secure components considering industrial risks.

, SP-SEC-Pgrm-5.2-8 - For infrastructure, the railway shall choose the location of secure components considering access and prevention of attacks to the location in case of major social events.

, SP-SEC-Pgrm-5.2-9 - For infrastructure, the railway shall define rules for choosing the location with respect of natural, environmental, and human-made disasters.

5.3 Commissioning and Maintenance

, SP-SEC-Pgrm-5.3-1 - The railway shall establish the commissioning process for each component including responsibilities for all parties involved.
Note: The according technical capabilities for commissioning and re-commissioning are defined in S P-SEC-Comp CH 5.5.4 PKI Commissioning Procedure

6 Configuration Management

, SP-SEC-Pgrm-6-1 - The railway shall implement configuration management using a configuration management tool to perform functionalities based on ISO 27002 chapter 8.9.

, SP-SEC-Pgrm-6-2 - The railway shall implement a change management process and change management tool to perform functionalities based on ISO 27002 chapter 8.32.

, SP-SEC-Pgrm-6-3 -

The change management process should be aligned to the Evolution Management Process.

6.1 Documentation

, SP-SEC-Pgrm-6.1-1 - The railway has the task to ensure that the railway system is sufficiently documented. Much of the documentation should be provided by or requested from the suppliers. The integration to a system overview is subject to the railway.

, SP-SEC-Pgrm-6.1-2 - The railway shall proof that all documentation is provided in electronic form.

, SP-SEC-Pgrm-6.1-3 - The railway shall proof that all documentation referenced in chapter 14.4 was provided.

, SP-SEC-Pgrm-6.1-4 - The railway shall ensure that all documentation is kept up to date.

7 Network and Communication Security

, SP-SEC-Pgrm-7-1 - The railway shall design the network segmenting the systems of the SuC from surrounding systems following the segregation principles of ISO 27002 chapter 8.22.

, SP-SEC-Pgrm-7-2 - The railway shall design the network so it can be disconnected from external networks of the SuC by using ISO 27002 chapter 8.20 and 8.21 as guiding support.

, SP-SEC-Pgrm-7-3 - The railway shall document the zones and network zone interconnections according to IEC 62443-2-1 Net 1.2.

Note: For the SuC, the zones and conduits model is presented in the Secure Component Specification. (4.2.3 Zone and conduits drawing)

, SP-SEC-Pgrm-7-4 - The railway shall follow IEC 62443-2-1 Net 1.4, where applicable.

, SP-SEC-Pgrm-7-5 - If systems and components implement a Human Machine interface, the railway shall ensure that only authorized, authenticated, encrypted and documented connections are used.

, SP-SEC-Pgrm-7-6 - For secure components, the Secure Component and Secure Communication specifications clearly define to only used authorized, authenticated, encrypted and documented connections. To ensure that any other system or component in the operational environment also applies this rule, the requirement is defined.

, SP-SEC-Pgrm-7-7 - If the secure component implements a Human Machine Interface, the railways shall configure the automatic termination time, unless it is an operator work place.

, SP-SEC-Pgrm-7-8 - The railway shall define a procedure how to manage log-in, log-out and screen lock at operator work places.]

, SP-SEC-Pgrm-7-9 - Operator work places are available onboard the train, e.g. the DMI and at the dispatcher and operator work places on the infrastructure side.

, SP-SEC-Pgrm-7-10 - Remote application access, beside the ones specified and referenced in Secure Component Specification, Shared Cybersecurity Specification, Secure Communication Specification, to the secure component shall not be implemented.

Note: Additional remote connections with a log-in to the device to any Secure Component are not necessary. All services are managed via central services of machine-to-machine connections, e.g. through the MDM.

, SP-SEC-Pgrm-7-11 - The railway shall define which additional communication interfaces beyond TSI/SP standardized interfaces shall be allowed based on the definition in the [SP-SEC-CompSpec].

, SP-SEC-Pgrm-7-12 - The railway shall ensure that, If the network is in a degraded state, the network management plane shall provide essential functionality.

Note: Essential functionality for network management is at minimum the possibility to monitor and configure the network devices. Software updated, for example, is not essential in this state.

, SP-SEC-Pgrm-7-13 - The railway shall implement policies and procedures to protect network accessible services applying the principles of ISO 27002 chapter 8.21.

, SP-SEC-Pgrm-7-14 - The railway shall hinder user-to-user messages by applying the principles of ISO 27002 chapter 8.20

, SP-SEC-Pgrm-7-15 - If the railway uses wireless networks, the railway shall apply policies and procedures by applying the principles of ISO 27002 chapter 8.20 and 8.21 for wireless networks.

, SP-SEC-Pgrm-7-16 - If the railway uses wireless networks, the railway shall segment the wireless network from the SuC following the segregation principles of ISO 27002 chapter 8.22.

, SP-SEC-Pgrm-7-17 - If the railway uses wireless networks, the railway shall implement policies and procedures according to Net 2.3.

8 Component Security

, SP-SEC-Pgrm-8-1 - If portable media has to be used, the railway shall apply ISO 27002 chapter 7.10 for managing portable media.

, SP-SEC-Pgrm-8-2 - The railway shall ensure that storage media containing software and configuration updates provide a visible identifier.

, SP-SEC-Pgrm-8-3 - The railway or supplier shall track the location of storage media containing software and configuration updates.

, SP-SEC-Pgrm-8-4 - The railway shall ensure that every secure component has access to its required Shared Cybersecurity Services defined in the Shared Cybersecurity Specification. SP-SEC-Pgrm-2.3-18 - [SP-SEC-ServSpec]

, SP-SEC-Pgrm-8-5 - The railway shall harden components prior to their use by applying the principles of ISO 27002 chapter 8.9.

, SP-SEC-Pgrm-8-6 - The suppliers are obliged to perform hardening according to Secure Component Specification chapter 5.3.6 Hardening.

, SP-SEC-Pgrm-8-7 - The railway shall require a confirmation by the supplier that the component is free of known malware before first use.

, SP-SEC-Pgrm-8-8 - The railway shall realize malware protection for secure components through allow listing.

, SP-SEC-Pgrm-8-9 - The railway shall define the allowlist to be used by the filter.
Note: Malware protection via virus scanner is not applied as it is not feasible in the OT domain.

, SP-SEC-Pgrm-8-10 - If malware protection shall be used for other than components than secure components, e.g. Shared Cybersecurity Services, the railway shall have policies and procedures related to malware protection availble based on ISO 27002 chapter 8.7.

8.1 Patch and Vulnerability Management

, SP-SEC-Pgrm-8.1-1 - The railway shall define legally binding responsibilities and duties for parties involved in the vulnerability management process of the component based on ISO 27002 chapter 8.8.

, SP-SEC-Pgrm-8.1-2 - The railway shall require the suppliers to follow a coordinated vulnerability disclosure procedure according to ISO 29147.

, SP-SEC-Pgrm-8.1-3 - The railway shall define procedures for the patch process of the secure component based on ISO 27002 chapter 8.32.

, SP-SEC-Pgrm-8.1-4 - The railway shall link the vulnerability management database to the configuration and software management database to allow the evaluation of the currently applied configurations and software considering potential vulnerabilities.

, SP-SEC-Pgrm-8.1-5 - The railway shall define procedures for the vulnerability management process of the component based on ISO 27002 chapter 8.8.

, SP-SEC-Pgrm-8.1-6 - The railway shall define procedures to evaluate the severity level of a vulnerability based on ISO 27002 chapter 8.29.

, SP-SEC-Pgrm-8.1-7 - The railway shall calculate the CVSS v4.0 Base + Threat + Environment metric for all vulnerabilities.

, SP-SEC-Pgrm-8.1-8 - The railway shall define a process to document and manage the risk (acceptance, mitigation, ...) based on ISO 27002 chapter 8.8 "taking appropriate measures to address technical vulnerabilities (i)", if an available patch is not installed .

, SP-SEC-Pgrm-8.1-9 - As evaluation basis commonly accepted methods or databases can be used. This is for example CVE. In addition railway application specifics are to be considered in scoring and respected for the evaluation and its process.

, SP-SEC-Pgrm-8.1-10 - The railway shall define procedures to evaluate the railway specific possible impact (criticality) for every vulnerability of installed hard- and software.

, SP-SEC-Pgrm-8.1-11 - The railway shall define a penetration testing strategy based on ISO 27002 chapter 8.8 (e).

, SP-SEC-Pgrm-8.1-12 - The railway shall follow the EUG Pentesting Guideline (EUG 23E245), where applicable.

, SP-SEC-Pgrm-8.1-13 - Penetration testing strategy means definitions like:

- testing intervals
- scoping
- depth of testing
- define roles and responsibility for fixing
- vulnerability fixing rules/policy

, SP-SEC-Pgrm-8.1-14 - The railway may use a test instance of the system under penetration testing including each component type for penetration testing.

, SP-SEC-Pgrm-8.1-15 - The railway shall use an automated test tool for security functionality verification of the system defined in the Secure Component Specification (5.7.2.6).

, SP-SEC-Pgrm-8.1-16 - The railway shall define a test strategy for security related testing before roll-out based on ISO 27002 chapter 8.29 and 8.31.

Note: Security related testing means functional tests for components and tests of the interoperability in the system context (integration testing) which focuses on the interface testing to ensure compatibility.

, SP-SEC-Pgrm-8.1-17 - The railway shall define a procedure to check the integrity and authenticity of software updates based on ISO 27002 chapter 8.29 and 8.31.

, SP-SEC-Pgrm-8.1-18 - The railway shall implement a process to check software before test and installation for malware based on ISO 27002 Chapter 8.7.

, SP-SEC-Pgrm-8.1-19 - Malware Detection is not installed in IACS systems. The target to protect against malware shall be reached by initial checks, integrity protection and security monitoring. Malware detection software would cause additional risks to the IACS system.

, SP-SEC-Pgrm-8.1-20 - Tracking of storage media is only needed as long as there is no network link between the railway's configuration database and the supplier's configuration database established. This is the target design and allows full traceability natively.

, SP-SEC-Pgrm-8.1-21 - The railway shall follow IEC 62443-2-1 DATA 1.3 for updating the secure component.

9 Protection of data

, SP-SEC-Pgrm-9-1 - The railway shall establish policies and procedures regarding classification and labeling of data based on ISO 27002 5.12 and 5.13.

, SP-SEC-Pgrm-9-2 - The railway shall use the Traffic Light Protocol (TLP) 2.0 for classifying information.

, SP-SEC-Pgrm-9-3 - The railway shall have policies and procedures related to confidentiality of data based on ISO 27002 5.14 and 5.15.

, SP-SEC-Pgrm-9-4 - The railway shall have policies and procedures regarding the configuration of safety systems based on ISO 27002 8.32.

, SP-SEC-Pgrm-9-5 - The railway shall have policies and procedures related to data retention based on ISO 27002 5.33.

, SP-SEC-Pgrm-9-6 - The Security Communication Specification defines which connection shall be secured by encryption and where the railway can choose based on the railways security policy. If the railway decides that encryption is not needed due to no need for data confidentiality, an integrity only cipher may be used.

, SP-SEC-Pgrm-9-7 - The railway shall implement IEC 62443-2-1 Data 1.5.

, SP-SEC-Pgrm-9-8 - The railway shall implement IEC 62443-2-1 Data 1.7.

9.1 Certificate Management

, SP-SEC-Pgrm-9.1-1 - The railway shall define an availability concept for the PKI including all sub services according to the overall system concept.

Note: The PKI system consists of multiple sub services that have different needs in operation concerning availability to serve the rail system. Details are available in the Shared Cybersecurity Services Specification.

, SP-SEC-Pgrm-9.1-2 - The root CA operation shall operate the root CA offline.

, SP-SEC-Pgrm-9.1-3 - Best practice for root CA operation is to keep it as default offline. Using an offline root CA makes compromising it nearly impossible. The root CA is only taken online to infrequently perform tasks such as (re)issuing issuing CA certificates or signing CRLs.

, SP-SEC-Pgrm-9.1-4 - The railway shall define the validity timespan of certificate revocation lists which was downloaded to the secure component.

, SP-SEC-Pgrm-9.1-5 - The railway shall define intervals for certificate validation according to operational need and security policy.

, SP-SEC-Pgrm-9.1-6 - The railway shall define and implement a process to revoke a certificate in a predetermined time.

Note: Certificates may be revoked due to different reasons in their foreseen life-time, e.g. a security incident occurs, a certificate was incorrectly assigned, ... To allow revocation of valid certificates via CRL, a process shall be in place to avoid unintended revocation of certificates that may lead to operational unavailability.

, SP-SEC-Pgrm-9.1-7 - If a component is decommissioned, the railway shall revoke any associated certificates.

, SP-SEC-Pgrm-9.1-8 - If the component is lost, the railway shall revoke any associated certificates.

, SP-SEC-Pgrm-9.1-9 - If a certificate is already expired, it does not need to be revoked in the decommissioning process. If the certificate is still valid, the certificate is revoked to exclude the possibility of making use of a stolen certificate.

Note: The secure component in this case is no CA or Root.

, SP-SEC-Pgrm-9.1-10 - The railway shall define the certificate validity for operator certificates according to the recommendations in the Shared Cybersecurity Services Specification (SP-SEC-SERV CH 14.1.2 Operator Certificate Profiles).

, SP-SEC-Pgrm-9.1-11 - The Railway operator shall install all for the installation relevant Manufacturer Root CA Certificates (MRCACs) in the PKI RA and network authentication server.

, SP-SEC-Pgrm-9.1-12 - Operators can restrict the services reachable by a secure component, if it is only authenticated with an MDC.

, SP-SEC-Pgrm-9.1-13 - The railway shall set the time for the request for renewing the certificate in advance to its expiration.

Note: Certificate validity and request for a new certificate are highly related to the rail system availability. Without a valid certificate, no connection can be established anymore. Best practice validity is 12 months. Best practice renewal request is three months before expiry (for 12 months valid certificates).

, SP-SEC-Pgrm-9.1-14 - If the ownership of a secure component shall be changed, the current owner shall perform the method Security:FactoryReset() as defined in SP-SEC-SERV 12.5-1 .

9.2 Decommissioning

, SP-SEC-Pgrm-9.2-1 - The railway shall document the decommissioning process.

, SP-SEC-Pgrm-9.2-2 - The railway shall require and establish procedures to securely purge data right after last usage for data stored on mobile or removable media and any other equipment capable of electronically store information.

, SP-SEC-Pgrm-9.2-3 - The railway shall require and establish procedures to securely destroy equipment if purging data is not possible.

, SP-SEC-Pgrm-9.2-4 - The railway shall revoke certificates of the component during decommissioning process.

, SP-SEC-Pgrm-9.2-5 - The railway shall remove all access rights of the component during decommissioning process.

, SP-SEC-Pgrm-9.2-6 - The railway shall change the status of the component in the asset management system to "to be decommissioned" before decommissioning process.

, SP-SEC-Pgrm-9.2-7 - The railway shall change the status of the component in the asset management system to "decommissioned" after successful decommissioning process.

, SP-SEC-Pgrm-9.2-8 - If the decommissioning process fails, the railway shall require a procedure to securely manage the component and prevent any electronic interaction with the system when decommissioning process can not be accomplished or fails.

, SP-SEC-Pgrm-9.2-9 - In case the decommissioning process fails, the following means could be used:

Placing security tamper-evident seals on the component interface and securely storing it until :

- actually performing the decommissionning process
- effectively destroying the device to prevent any reuse of its data storage.

, SP-SEC-Pgrm-9.2-10 - The railway shall define decommission procedures ensuring stopping the security monitoring of the component.

10 User access control

, SP-SEC-Pgrm-10-1 - The railway shall follow the least privilege principle for assigning users and roles.

, SP-SEC-Pgrm-10-2 - The railway shall assign roles to functions of the secure components using the IAM (Identity and Access Management) based on ISO 27002 chapter 5.16 and 5.15.

, SP-SEC-Pgrm-10-3 - The railway shall define rules for deletion of all access rights for users that do not or no longer need access.

, SP-SEC-Pgrm-10-4 - The railway shall define for which users automatic disabling of access rights shall not apply.

, SP-SEC-Pgrm-10-5 - The railway shall define a process, including frequency, for regular check of all access rights concerning their need and validity based on ISO 27002 5.18.

, SP-SEC-Pgrm-10-6 - The railway shall assign users to roles in the IAM.

, SP-SEC-Pgrm-10-7 - The railway shall assign permissions to roles in the IAM.

, SP-SEC-Pgrm-10-8 - The railway shall define a re-certification process for users.

, SP-SEC-Pgrm-10-9 - Users mean here according to IEC 62443-2-1 human users, software processes or devices. Usually, the expression "identity" is used in this context. The access rights are assigned to roles, which users then inherit from the roles that have been assigned to them.

, SP-SEC-Pgrm-10-10 - The railway shall define the interval of the certificates validity check related to SP-SEC-Serv CH 14.1.2 - Operator Certificate Profiles on secure component level.

, SP-SEC-Pgrm-10-11 - The railway shall define the interval of regular checks for the requirements based on ISO 27002 chapter 5.16 and 5.15 based on a risk analysis.

, SP-SEC-Pgrm-10-12 - Adaption of roles and permissions shall be analysed concerning the impact on user access rights.

Note: Adaption of roles and permissions may lead to toxic access rights for users, for example the right to sign for creation and approval of configuration files. To avoid such unintentional combinations, every change in permissions and roles needs to be analysed accordingly.

, SP-SEC-Pgrm-10-13 - The railway shall grant physical access based on the least-privilege-principle.

, SP-SEC-Pgrm-10-14 - The railway shall apply policies and procedures to identify and authenticate the defined software services defined in the Secure Component Specification.

, SP-SEC-Pgrm-10-15 - The railway shall deny interactive login capabilities for technical identities.

, SP-SEC-Pgrm-10-16 - The railway shall ensure that every user (human users, software processes or devices) is a unique identity.

, SP-SEC-Pgrm-10-17 - If a human access is available, multi factor authentication for the human users shall be used as defined in SP-SEC-COMP 7.2-1 using SSI-UAS.

, SP-SEC-Pgrm-10-18 - The railway shall apply procedures and policies to use the mutual authentication mechanisms defined in the Secure Component Specification.

, SP-SEC-Pgrm-10-19 - The railway shall define roles following the segregation of duties principle.

, SP-SEC-Pgrm-10-20 - If passwords are used, the railway shall provide the applicable password policies based on ISO 27002 5.17.

Note: Password policies include, amongst others, its minimum number of characters, complexity and validity end-date. Unless no information of compromised password, the password should not be changed.

Note: The default configuration should be that the validity end-date is not used (unlimited validity).

, SP-SEC-Pgrm-10-21 - The railway shall establish password policies and procedures for human users based on ISO 27002 chapter 5.7.

, SP-SEC-Pgrm-10-22 - Password rules are not applicable for machine-machine interfaces.

, SP-SEC-Pgrm-10-23 - The railway shall establish a procedure and policy to manage disclosed/compromised passwords according to IEC 62443-2-1 User 1.12.

, SP-SEC-Pgrm-10-24 - Requirement IEC 62443-2-1 User 1.13 is implemented by .SP-SEC-COMP 7.2-8

, SP-SEC-Pgrm-10-25 - Requirement IEC 62443-2-1 User 1.13 is implemented by SP-SEC-COMP 7.2-9

, SP-SEC-Pgrm-10-26 - The railway shall ensure unique user identification by denying shared credentials.

, SP-SEC-Pgrm-10-27 - The railway shall define policies and procedures related to separation of duties based on ISO 27002 5.3

, SP-SEC-Pgrm-10-28 - The railway shall define critical functions and related tasks which require the implementation of the multiple approvals (dual approval) principle.

Note: Critical functions are, e.g.:

- Changes of configuration
- Deployment of new software versions
- Managing of authorisations and permissions

, SP-SEC-Pgrm-10-29 - The railway shall have policies and procedures related to multiple approvals based on security requirements based on ISO 27002 8.26

, SP-SEC-Pgrm-10-30 - The railway shall have procedures and policies in the IAM to deny login

access according to IEC 62443-2-1 User 1.15.

, SP-SEC-Pgrm-10-31 - The railway shall define policies to use the procedures provided by the secure component (Secure Component Specification chapter 7.2) for session integrity.
Note: The definitions of roles, duties and rights are usually defined in a "User Access Policy".

, SP-SEC-Pgrm-10-32 - Usually the automatic access right disabling should not be used for users that are directly managing the railway operation. This counts for example for CCC operators, train drivers or dispatchers and for admins that are handling access rights. For these user categories automatic access disabling may cause catastrophic availability issues.Automatic process in this context means that the IAM's system shall automatically address a third person to decide whether the user shall remain having access or not.
For standard users, the access rights are automatically revoked, if they are not approved in time.
For persistent users, the accounts stay valid until active approval of revocation.

, SP-SEC-Pgrm-10-33 - The railway shall establish a process to configure the maximum allowed concurrent sessions based on Secure Component Specification 5.4.4-4.

, SP-SEC-Pgrm-10-34 - The railway shall define policies and procedures regarding access rights based on ISO 27002 8.3

, SP-SEC-Pgrm-10-35 - The railway shall have policies and procedures related to the elevation of privileges for access based on ISO 27002 8.2.

11 Event and incident management

, SP-SEC-Pgrm-11-1 - The railway shall implement a vulnerability management database based on ISO 27002 chapter 8.8.

Note: The vulnerability management database is filled based on the input by the suppliers concerning their bill of material.

, SP-SEC-Pgrm-11-2 - The railway shall implement a vulnerability management process.

, SP-SEC-Pgrm-11-3 - The railway should define a vulnerability scanning strategy for each component type.

Note: Components differ concerning their interfaces, accessibility, etc. Components may be grouped in to different types that can be treated in the same way. This categorisation is meant with "component type".

Scanning strategy means definitions like:

- scanning intervals
- scoping
- define roles and responsibility for fixing
- vulnerability fixing rules/policy

, SP-SEC-Pgrm-11-4 - Vulnerability scanning of components can be performed in test environments. That reduces costs and possible negative effects on the productive system.
A typical repetition time for vulnerability scanning in practice is any major releases or every two years.

, SP-SEC-Pgrm-11-5 - The railway shall define a logging strategy, integrating legacy and new systems.

, SP-SEC-Pgrm-11-6 - The railway shall follow the EUG (ERTMS Users Group) logging guideline 23E177 (version 1A), where applicable.

, SP-SEC-Pgrm-11-7 - The railway shall define logging requirements based on ISO 27002 chapter 8.15.

, SP-SEC-Pgrm-11-8 - The railway shall ensure a centrally managed system-wide audit trail is implemented according to IEC 62443-3-3 SR 2.8 RE 1 in the central SOC.

, SP-SEC-Pgrm-11-9 - The railway shall define policies and procedures to protect the security logs applying the measures of ISO 27002 chapter 5.33.

, SP-SEC-Pgrm-11-10 - The railway shall define policies and procedures for event analysis according to chapters 5.25, 5.26 and 6.8.

, SP-SEC-Pgrm-11-11 - The railway shall integrate the logs of the Secure Components provided based on the Secure Component Specification chapter 5.7.

, SP-SEC-Pgrm-11-12 - The railway shall apply the defined interfaces by the Secure Communication and Shared Cybersecurity Specification to report events.

, SP-SEC-Pgrm-11-13 - The railway shall define an incident handling and response process

based on ISO 27002 chapter 5.26.

, SP-SEC-Pgrm-11-14 - The railway shall regularly test the incident management process.

Note: The regular testing of the incident management and response process should be performed on a yearly basis.

, SP-SEC-Pgrm-11-15 - For European wide exchange of information about incidents and threats a collaboration platform is set up. The project is called RAIL ISAC. Information about the status and participation can be gathered on https://rail-isac.eu/ .

12 System integrity and availability

, SP-SEC-Pgrm-12-1 - The railway shall customise the railway's availability concept for project specific specialties.

Note: The availability concept should take redundancy and geo-redundancy into account depending on the availability requirements and possible failures of the system. The failure analysis is also linked to the overall disaster recovery plan which may require certain redundancy.

, SP-SEC-Pgrm-12-2 - The railway shall consider the potential maximum number of connections that will use the Shared Cybersecurity Services with respect to scalability during design.

, SP-SEC-Pgrm-12-3 - The railway shall align the overall system RAM (Reliability, Availability, Maintainability) target with the security availability concept.

Note: The availability concept for security analyses the possible impact on the system availability, if security services fail. Based on this analysis the availability requirements for these services are defined. The availability targets may differ between the different services. The availability of the secure components themselves is mainly covered by the RAM target of the overall system concept as security are normally integrated functions and no separate components inside the secure component.

12.1 Business Continuity Management (BCM)

, SP-SEC-Pgrm-12.1-1 - The railway shall define and implement a disaster recovery plan.

, SP-SEC-Pgrm-12.1-2 - The railway shall test the disaster recovery plan in a self defined repetition rate.

, SP-SEC-Pgrm-12.1-3 - The railway shall have a continuity management based on ISO 27002 5.30

, SP-SEC-Pgrm-12.1-4 - The railway shall have a resource availability and redundancy management based on ISO 27002 8.14

, SP-SEC-Pgrm-12.1-5 - The railway shall have policies and procedures for controlling the security and functionality during a failure-state based on ISO 27002 5.29

, SP-SEC-Pgrm-12.1-6 - The railway and supplier should establish an escrow agreement to protect from bankruptcy or market exit of the supplier.

12.2 Time

, SP-SEC-Pgrm-12.2-1 - The railway shall define availability requirements for SSS-STS (Secure Time Synchronisation) and ESS-TIME according to the overall system concept.

, SP-SEC-Pgrm-12.2-2 - The railway shall define a time source hierarchy concept based on the requirements in SP-SEC-SERV CH 5

, SP-SEC-Pgrm-12.2-3 - The railway shall distribute time securely as defined in the Shared Cybersecurity Specification SP-SEC-SERV CH 5

, SP-SEC-Pgrm-12.2-4 - Time sources within the railway should rely to a common time source of UTC as defined in the shared security services specification. The hierarchy concept helps to respect different availability and protection needs of different components and systems in the overall railway system.

12.3 Backup and Restore

, SP-SEC-Pgrm-12.3-1 - The railway shall have policies and procedures for backup and restore based on ISO 27002 8.13

, SP-SEC-Pgrm-12.3-2 - The railway shall ensure that the back-up procedures do not adversely affect normal railway operation according to IEC 62443-2-1 Avail 2.2.

, SP-SEC-Pgrm-12.3-3 - The railway shall have the possibility to do Bare-Metal-Restore for all systems.

, SP-SEC-Pgrm-12.3-4 - Backup shall be performed with a central system.

, SP-SEC-Pgrm-12.3-5 - The restore process shall be managed by a central system.

, SP-SEC-Pgrm-12.3-6 - Backup of software, configuration and log data is not performed at the end points, like the interlocking, field element controller or EVC. The back-up is centrally organised by storing all of the relevant data (configuration, software) prior to the installation for restore processes. Logging data (security and diagnostic) is also stored centrally. The foreseen central service is the MDM. Further details are defined in the Shared Cybersecurity Services specification.

13 Suppliers

13.1 Organisational Requirements

, SP-SEC-Pgrm-13.1-1 - The supplier shall establish and maintain ISO 27001 certification for the development organisation.

, SP-SEC-Pgrm-13.1-2 - The supplier shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10.

, SP-SEC-Pgrm-13.1-3 - The supplier shall establish and maintain IEC 62443-4-1 minimum ML 3 certification for the secure development lifecycle of the secure components.

, SP-SEC-Pgrm-13.1-4 - The service provider shall be certified according to ISO 27001 for the organisation.

, SP-SEC-Pgrm-13.1-5 - The service provider shall establish and maintain IEC 62443-2-4 minimum ML 3 certification for the service provided.

, SP-SEC-Pgrm-13.1-6 - ML 3 refers to Level 3 of the Capability Maturity Model Integration (CMMI) defined in IEC 62443-4-1 and IEC 62443-2-4.

, SP-SEC-Pgrm-13.1-7 - The supplier shall perform background checks for personnel that has access to any part of the system under consideration defined in Security Architecture in the whole life-cycle (from development to decommissioning).
Note: Recommended activities for background checks are documented in ISO 27002 chapter 6.1.

, SP-SEC-Pgrm-13.1-8 - The supplier shall provide a single point of contact for the exchange of security related information.

13.2 Supply Chain

, SP-SEC-Pgrm-13.2-1 - This chapter shall give additional guidance for security for the secure delivery of components and contractual basis the railway should require to support this. The target of these measures is to avoid a manipulation of the systems from production to commissioning.

, SP-SEC-Pgrm-13.2-2 - The supplier should implement supply chain security management.
Note: Recommended activities for supply chain management are document in IEC 52443-4-1 (SM-9, SM-10) and ISO 27002 5.21.

, SP-SEC-Pgrm-13.2-3 - The supplier shall seal the transport container using tamper-evident seals so manipulation is indicated.

, SP-SEC-Pgrm-13.2-4 - The supplier shall define the tamper evident seal for the container based on the assumed risk.

, SP-SEC-Pgrm-13.2-5 - The definition and the risk assumption shall be documented and communicated to the customer prior to delivery.

, SP-SEC-Pgrm-13.2-6 - The supplier shall track transport steps incl. means of transport and storage time and location starting from shipping from the suppliers location.

, SP-SEC-Pgrm-13.2-7 - If applicable by law and if suppliers have access to any part of the system under consideration defined in Security Architecture in the whole life-cycle (from development to decommissioning), the supplier shall perform personnel background security checks for this personnel

Note: Recommend activities for background checks are documented in ISO 27002 chapter 6.1. [IEC 62443-2-4 SP.01.04]

13.3 Patch and Vulnerability Management

13.3.1 Vulnerability Notifications

, SP-SEC-Pgrm-13.3.1-1 - The manufacturer shall submit an early warning notification to the designated CSIRT, ENISA and to affected customers of actively exploitable vulnerabilities in Secure Components without undue delay and within 24h of becoming aware of it.

See IEC 62443-4-1 DM-5 - Disclosing security-related issues for details of disclosed information including additional potential cross-borders impacts.

, SP-SEC-Pgrm-13.3.1-2 - Affected customer is a customer who operates the product.

, SP-SEC-Pgrm-13.3.1-3 - The manufacturer shall submit a vulnerability information to the the d esignated CSIRT, ENISA and affected customers of actively exploited vulnerabilities in Secure Components with undue delay and within of 72h of becoming aware of it.

, SP-SEC-Pgrm-13.3.1-4 - The manufacturer shall submit a final report to the the designated CS IRT and to ENISA and to affected customers of actively exploited vulnerabilities in Secure Components no later than 14 days after a corrective or mitigation measure is available.

, SP-SEC-Pgrm-13.3.1-5 - The supplier shall calculate and communicate the vulnerability score using the CVSS 4.0 Base + Threat metric.

, SP-SEC-Pgrm-13.3.1-6 - The supplier shall communicate any new information affecting to the CVSS 4.0 Base + Threat metric of a vulnerability to the railway without undue delay.

13.3.2 Incident Notifications

, SP-SEC-Pgrm-13.3.2-1 - The manufacturer shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at manufacturer which has impact on the security of the Secure Component including at least suspicion of unlawful or malicious acts, and affected Member States.

Note: incident in this context is a successful security breach at the manufacturer

Note: a severe incident is defined to have a negative impact on availability, authenticity, integrity or confidentiality of sensitive or important data or functions or allows execution of malicious code

, SP-SEC-Pgrm-13.3.2-2 - The manufacturer shall submit an incident notification within 72h to the designated CSIRT and to ENISA of any severe incident at manufacturer which has impact on the security of the Secure Component including general information of the nature of the event, initial assessment of the incident, sensitivity of notification, and any corrective or mitigating measures.

, SP-SEC-Pgrm-13.3.2-3 - The manufacturer shall submit a final report within one month to the designated CSIRT and to ENISA of any severe incident at manufacturer which has impact on the security of the Secure Component including detailed description, severity, impact, type of threat or root cause, applied and ongoing mitigation measures.

, SP-SEC-Pgrm-13.3.2-4 - The manufacturer shall notify without undue delay and after becoming aware, the impacted user of the Secure Component of the incident, including when necessary, corrective measures for mitigating the impact of the incident.

, SP-SEC-Pgrm-13.3.2-5 - The supplier shall implement processes for discovery of security anomalies and network security.

Note: recommended activities for discovery of security anomalies are documented in ISO 27002 8.16 (monitoring activities) and 8.20 (network security)

13.3.3 Update Distribution

, SP-SEC-Pgrm-13.3.3-1 - The manufacturer shall provide for mechanisms to securely distribute updates for Secure Components (e.g. using the updated package defined in SP-SEC-CompSpec Ch 5.6.2 - Update package).

, SP-SEC-Pgrm-13.3.3-2 - The manufacturer shall provide the security patches or updates without delay accompanied by advisory messages providing users with the relevant information, including on potential actions to be taken.

, SP-SEC-Pgrm-13.3.3-3 - The manufacturer shall ensure that the security patches or updates made available to users during the support periods remains available after it has been issued for a minimum of 10 years or the for the remainder of the support period, whichever is longer.

, SP-SEC-Pgrm-13.3.3-4 - If a manufacturer ceases its operation, the manufacturer shall inform the relevant market authorities and the users of the affected products about this situation.

, SP-SEC-Pgrm-13.3.3-5 - The supplier shall document the changes introduced by the security patches/updates and provide argumentation that it does not affect the safety functionality (e.g. minimal change case).

Note: The conditions to argue a minimal change of the security functionality can encompass software, configuration and parameterization data, certificates changes...

, SP-SEC-Pgrm-13.3.3-6 - If a new patch or update causes a reduction in the security of the component due to technical reasons, the supplier informs the railway with the delivery about this reduction in the security of the component and possible mitigation (see IEC 62443-4-1 SUM-2).

, SP-SEC-Pgrm-13.3.3-7 - The supplier shall provide storage media containing software and configuration updates only with a visible identifier.

13.4 Technical Documentation and Bill of Material

, SP-SEC-Pgrm-13.4-1 - The supplier shall create technical documentation for each supplied component according to the requirements in SP-SEC-CompSpec Ch 6.3 - Product Documentation

, SP-SEC-Pgrm-13.4-2 - The supplier shall make the Secure Component technical documentation accessible for market surveillance authorities for ten years after the component has been put on the market or for the support period, whichever is longer.

Note: market surveillance authorities as defined in EU 2022/0272 CRA

, SP-SEC-Pgrm-13.4-3 - The supplier shall create a software bill of materials using the CycloneDX SBOM standard containing at least the top-level dependencies of the Secure Component.

Note 1: CycloneDX SBOM standard is machine-readable and human-readable.

Note 2: Top-level dependencies of a Secure Component are the main identifiable and exchangeable sub-components (e.g. for an embedded component: firmware version, essential application version) for which a dedicated vulnerability management information exists..

, SP-SEC-Pgrm-13.4-4 - The software bill of material shall contain at least the data fields defined in SP-SEC-Pgrm-2.3-10 - [MinElements SBOM]

, SP-SEC-Pgrm-13.4-5 - The service provider shall provide reference pictures of the secure components and their installation places to allow visual inspection for commissioning by the railways.

13.5 User Management

, SP-SEC-Pgrm-13.5-1 - The supplier shall provide a default role to permissions mappings for each supplied component.

Note: Recommended policies and procedures regarding access rights are documented in ISO 27002 chapter 8.3.