EU-RAIL SYSTEM PILLAR

Regulatory Compliance

Version: 1.1.1

Regulatory Compliance

Document data

Created by	System Pillar Cybersecurity Domain
Classification	Public
Status	Released
Version	1.1.1
Date	28-OCT-2026

Copyright

© Europe's Rail Joint Undertaking, 2026

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 authorises you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following: EU Rail trade mark, title of the document, year of publication, version of document.

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 trade marks 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.

DRAFT

Document History

Version	Date	Description	Status
1.1.1	28-OCT-2026	Release for ERA Technical Documents	released
1.1	23-MAR-2026	Error correction and additional guidance for version 1.0	released
1.0	20-FEB-2025	Initial public release	released

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

DRAFT

1 Table of Contents

1 Table of Contents 4
2 About this Document 5
2.1 About this Document 5
3 EU Cybersecurity regulations 7
3.1 EU-NIS2 compliance 7
3.2 EU-CSA compliance 20
3.3 EU-CRA compliance 79
3.4 EU-RED compliance 160
4 International standards 163
4.1 IEC 62443-2-1 (2024) compliance 163
4.2 IEC 62443-4-2 compliance 186
4.2.1 Rationale for not considered requirements from IEC 62443-4-2 186
4.2.2 Tracing to IEC 62443-4-2 188
4.3 CLC/TS 50701 compliance 240
4.4 IEC PT 63452 compliance 245

DRAFT

2 About this Document

2.1 About this Document

This documents contains the tracing tables to EU cybersecurity legislation:

- NIS 2
- Cybersecurity Act
- Cyber Resilience Act
- Radio Equipment Directive

and international standards:

- IEC 62443-2-1
- IEC 62443-4-2
- CENELEC CLC/TS 50701
- IEC PT 63452 (draft status Jan 2025)

DRAFT

DRAFT

3 EU Cybersecurity regulations

3.1 EU-NIS2 compliance

Table containing NIS2 req no, title and corresponding req or chapter in this doc.

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-20-1	Approval of cybersecurity risk-management measures	1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article. The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.	_ is implemented by: SP-SEC-Pgrm-5-12: The railway shall have policies and procedures for the management of risks based on ISO 27001 6.1. _ is implemented by: SP-SEC-Pgrm-5-2: The railway shall ensure that the railway management bodies approve the cybersecurity risk-management measures.
EU-NIS2-20-2	Training of management body and employees	2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	_ is implemented by: SP-SEC-Pgrm-5-10: The railway shall establish a security awareness and training program based on ISO 27002 chapter 6.3.

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-21-1	Take technical, operational and organisational measures	1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services. Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.	_ is implemented by: EU-NIS2-21-3: 3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

DRAFT

EU-NIS2-21-2	All-hazard approach	2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following (a) policies on risk analysis and information system security (b) incident handling; (c) business continuity, such as backup management and disaster recovery, and crisis management; (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers; (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure; (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures; (g) basic cyber hygiene practices and cybersecurity training; (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption; (i) human resources security, access control policies and asset management; (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	_ is implemented by: 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. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-8.1-5: The railway shall define procedures for the vulnerability management process of the Secure Component based on ISO 27002 chapter 8.8. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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). _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-8.1-17: The

DRAFT

			railway shall define a procedure to check the integrity and authenticity of software updates based on ISO 27002 chapter 8.29 and 8.31. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-8.1-11: The railway shall define a penetration testing strategy based on ISO 27002 chapter 8.8 (e).

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-21-3	Supply chain vulnerability management	3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).	_ is implemented by: SP-SEC-Pgrm-13.3.2-1: The supplier shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at supplier 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 supplier. 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

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-21-4	Corrective measures	4. Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.	_ is implemented by: EU-NIS2-21-3: 3. Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

DRAFT

EU-NIS2-23-1	Incident reporting	1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt. In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.	_ is implemented by: EU-NIS2-23-2: 2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself. _ is implemented by: SP-SEC-Pgrm-13.3.2-1: The supplier shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at supplier 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 supplier. 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 _ is implemented by: SP-SEC-Pgrm-13.3.2-2: The supplier shall submit an incident notification within 72h to the designated CSIRT and to ENISA of any severe incident at supplier 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.

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-23-2	Report measures or remedies to service recipients	2. Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.	_ is implemented by: SP-SEC-Pgrm-13.3.2-1: The supplier shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at supplier 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 supplier. 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

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-23-3	Significant incident	3. An incident shall be considered to be significant if: (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned; (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.	_ is implemented by: 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.

DRAFT

EU-NIS2-23-4	CSIRT reporting	4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority: (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates; (d) a final report not later than one month after the submission of the incident notification under point (b), including the following: 1. (i) a detailed description of the incident, including its severity and impact 2. (ii) the type of threat or root cause that is likely to have triggered the incident; 3. (iii) applied and ongoing mitigation measures; 4. (iv) where applicable, the cross-border impact of the incident;	_ is implemented by: SP-SEC-Pgrm-13.3.1-1: The supplier shall submit an early warning notification to the designated CSIRT, ENISA and to affected customers of actively exploited 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.

DRAFT

		(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident. By way of derogation from the first subparagraph, point (b), a trust service provider shall, with regard to significant incidents that have an impact on the provision of its trust services, notify the CSIRT or, where applicable, the competent authority, without undue delay and in any event within 24 hours of becoming aware of the significant incident.	

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-24-1	Use of certified products	1. In order to demonstrate compliance with particular requirements of Article 21, Member States may require essential and important entities to use particular ICT products, ICT services and ICT processes, developed by the essential or important entity or procured from third parties, that are certified under European cybersecurity certification schemes adopted pursuant to Article 49 of Regulation (EU) 2019/881. Furthermore, Member States shall encourage essential and important entities to use qualified trust services.	_ is implemented by: : [SP-SEC-CompSpec] _ is implemented by: : [SP-SEC-CommSpec]
EU-NIS2-25-1	Use of European and international standards	1. In order to promote the convergent implementation of Article 21(1) and (2), Member States shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European and international standards and technical specifications relevant to the security of network and information systems.	_ is implemented by: SP-SEC-Pgrm-13.1-2: The supplier shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-13.1-1: The supplier shall establish and maintain ISO 27001 certification for the development organisation.

DRAFT

EU NIS2	Topic	Requirement	Implemented by
EU-NIS2-25-2	Guidelines for standards	2. ENISA, in cooperation with Member States, and, where appropriate, after consulting relevant stakeholders, shall draw up advice and guidelines regarding the technical areas to be considered in relation to paragraph 1 as well as regarding already existing standards, including national standards, which would allow for those areas to be covered.	_ is implemented by: 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.
13 items found			

3.2 EU-CSA compliance

The table contains the CSA requirement no, title and corresponding requirement or chapter in this document.

Two aspect of the requirements are not considered in this version of the specifications: statement of conformity and assurance levels. These aspects will be added once a decision is made by the rail (automation) sector to create a European cybersecurity certification scheme for rail (automation) products.

DRAFT

EU-CSA-51 a	Confidentiality	(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure durin

DRAFT

DRAFT

EU-CSA-51 b	Integrity and Availability	(b) to protect stored, transmitted or otherwise processed data against accidental or unauthorised destruction, loss or alteration or lack of availabil

DRAFT

DRAFT

DRAFT

DRAFT

EU-CSA-51 c	Authentication and Authorization	(c) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;

DRAFT

DRAFT

EU-CSA-51 d	Vulnerability Management	(d) to identify and document known dependencies and vulnerabilities;

DRAFT

DRAFT

DRAFT

EU-CSA-51 e	Security logging	(e) to record which data, services or functions have been accessed, used or otherwise processed, at what times and by whom;

DRAFT

DRAFT

EU-CSA-51 f	Non-repudiation	(f) to make it possible to check which data, services or functions have been accessed, used or otherwise processed, at what times and by whom

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51 g	Vulnerability testing	(g) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;

DRAFT

EU CSA	Topic	Requirement

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51 h	Backup and restore	(h) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;

DRAFT

EU-CSA-51 i	Secure-by-default	(i) that ICT products, ICT services and ICT processes are secure by default and by design;

DRAFT

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51 j-1	Free from publicly known vulnerabilities	(j) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vul

DRAFT

EU-CSA-51 j-2	Security update functionality	and are provided with mechanisms for secure updates

DRAFT

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51-2	Reference to assurance level	European cybersecurity certificates and EU statements of conformity shall refer to any assurance level specified in the European cybersecurity c
EU-CSA-51-3	Scheme requirements	The security requirements corresponding to each assurance level shall be provided in the relevant European cybersecurity certification scheme,
EU-CSA-51-4	Technical specification reference	The certificate or the EU statement of conformity shall refer to technical specifications, standards and procedures related thereto, including techn

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51-5	Assurance level: Basic	A European cybersecurity certificate or EU statement of conformity that refers to assurance level ‘basic’ shall provide assurance that the ICT proc

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51-6	Assurance level: Substantial	A European cybersecurity certificate that refers to assurance level ‘substantial’ shall provide assurance that the ICT products, ICT services and IC correctly implement the necessary security functionalities. Where any such evaluation activities are not appropriate, substitute evaluation activitie

DRAFT

EU-CSA-51-7	Assurance level: High	A European cybersecurity certificate that refers to assurance level ‘high’ shall provide assurance that the ICT products, ICT services and ICT pro tionalities at the state of the art; and an assessment of their resistance to skilled attackers, using penetration testing. Where any such evaluation

DRAFT

EU CSA	Topic	Requirement
EU-CSA-51-8	Multiple assurance levels	A European cybersecurity certification scheme may specify several evaluation levels depending on the rigour and depth of the evaluation method
EU-CSA-52-1	Assurance levels	A European cybersecurity certification scheme may specify one or more of the following assurance levels for ICT products, ICT services and ICT

DRAFT

EU CSA	Topic	Requirement
EU-CSA-53-1	Self-assessment for assurance level Basic	A European cybersecurity certification scheme may allow for the conformity self-assessment under the sole responsibility of the manufacturer or
EU-CSA-53-2	EU statement of conformity	The manufacturer or provider of ICT products, ICT services or ICT processes may issue an EU statement of conformity stating that the fulfilment

DRAFT

EU CSA	Topic	Requirement
EU-CSA-53-3	Availability of supporting information	The manufacturer or provider of ICT products, ICT services or ICT processes shall make the EU statement of conformity, technical documentatio
EU-CSA-54-1a	Scope	(a) the subject matter and scope of the certification scheme, including the type or categories of ICT products, ICT services and ICT processes co

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1b	Purpose	(b) a clear description of the purpose of the scheme and of how the selected standards, evaluation methods and assurance levels correspond to
EU-CSA-54-1c	Referenced standards	(c) references to the international, European or national standards applied in the evaluation or, where such standards are not available or approp
EU-CSA-54-1d	Assurance levels	(d) where applicable, one or more assurance levels;

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1e	Self-assessment	(e) an indication of whether conformity self-assessment is permitted under the scheme;
EU-CSA-54-1f	Technical competence of conformity assessment bodies	(f) where applicable, specific or additional requirements to which conformity assessment bodies are subject in order to guarantee their technical c
EU-CSA-54-1g	Evaluation criteria	(g) the specific evaluation criteria and methods to be used, including types of evaluation, in order to demonstrate that the security objectives refe

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1h	Required documentation	(h) where applicable, the information which is necessary for certification and which is to be supplied or otherwise be made available to the confor
EU-CSA-54-1i	Marks and Labels	(i) where the scheme provides for marks or labels, the conditions under which such marks or labels may be used;
EU-CSA-54-1j	Compliance monitoring rules	(j) rules for monitoring compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certifica

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1k	Certificate conditions	(k) where applicable, the conditions for issuing, maintaining, continuing and renewing the European cybersecurity certificates, as well as the cond
EU-CSA-54-1l	Unconformity consequences	(l) rules concerning the consequences for ICT products, ICT services and ICT processes that have been certified or for which an EU statement o

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1m	Vulnerability disclosure	(m) rules concerning how previously undetected cybersecurity vulnerabilities in ICT products, ICT services and ICT processes are to be reported
EU-CSA-54-1n	Record retention	(n) where applicable, rules concerning the retention of records by conformity assessment bodies;

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1o	Similar schemes	(o) the identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products, ICT ser
EU-CSA-54-1p	Certificate content and format	(p) the content and the format of the European cybersecurity certificates and the EU statements of conformity to be issued;
EU-CSA-54-1q	Availability period	(q) the period of the availability of the EU statement of conformity, technical documentation, and all other relevant information to be made availab
EU-CSA-54-1r	Maximum validity period	(r) maximum period of validity of European cybersecurity certificates issued under the scheme;

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1s	Certificate disclosure policy	(s) disclosure policy for European cybersecurity certificates issued, amended or withdrawn under the scheme;
EU-CSA-54-1t	Mutual recognition with third countries	(t) conditions for the mutual recognition of certification schemes with third countries;
EU-CSA-54-1u	Peer assessment	(u) where applicable, rules concerning any peer assessment mechanism established by the scheme for the authorities or bodies issuing Europea

DRAFT

EU CSA	Topic	Requirement
EU-CSA-54-1v	ICT products, services and processes	(v) format and procedures to be followed by manufacturers or providers of ICT products, ICT services or ICT processes in supplying and updatin
EU-CSA-54-2	Legal compliance	2. The specified requirements of the European cybersecurity certification scheme shall be consistent with any applicable legal requirements, in p

DRAFT

EU-CSA-55-1a	Security manuals	(a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the

DRAFT

DRAFT

EU CSA	Topic	Requirement
EU-CSA-55-1b	Period of security support	(b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity related updates;
EU-CSA-55-1c	Contact information	(c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security
EU-CSA-55-1d	Online vulnerability information	(d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any rel

DRAFT

EU CSA	Topic	Requirement
EU-CSA-55-2	Electronic form	2. The information referred to in paragraph 1 shall be available in electronic form and shall remain available and be updated as necessary at leas
EU-CSA-56-1	Compliance to requirements	1. ICT products, ICT services and ICT processes that have been certified under a European cybersecurity certification scheme adopted pursuant
EU-CSA-56-2	Voluntary or mandatory	2. The cybersecurity certification shall be voluntary, unless otherwise specified by Union law or Member State law.

DRAFT

EU-CSA-56-3	Efficiency assessment	3. The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a spe an existing certification scheme which are to be covered by a mandatory certification scheme. As a priority, the Commission shall focus on the sectors listed in Annex II to Directive (EU) 2016/1148, which shall be assessed at the latest two y

DRAFT

EU CSA	Topic	Requirement
EU-CSA-56-4a	Conformity assessment bodies duties	4. The conformity assessment bodies referred to in Article 60 shall issue European cybersecurity certificates pursuant to this Article referring to assurance level ‘basic’ or ‘substantial’ on the basis of criteria included in the European cybersecurity certification scheme adopted by the Commission pursuant to Article 49.

DRAFT

EU CSA	Topic	Requirement
EU-CSA-56-5	Assessment bodies requirements	5. By way of derogation from paragraph 4, in duly justified cases a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by a public body. Such body shall be one of the following: (a) a national cybersecurity certification authority as referred to in Article 58(1); or (b) a public body that is accredited as a conformity assessment body pursuant to Article 60(1).

DRAFT

EU CSA	Topic	Requirement
EU-CSA-56-6	Assessment bodies requirement for assurance level "High"	6. Where a European cybersecurity certification scheme adopted pursuant to Article 49 requires an assurance level ‘high’, the European cyberse (a) upon prior approval by the national cybersecurity certification authority for each individual European cybersecurity certificate issued by a conf (b) on the basis of a general delegation of the task of issuing such European cybersecurity certificates to a conformity assessment body by the n

DRAFT

EU CSA	Topic	Requirement
EU-CSA-56-7	Required information	7. The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the national cybe

DRAFT

EU CSA	Topic	Requirement
EU-CSA-56-8	Vulnerability information	8. The holder of a European cybersecurity certificate shall inform the authority or body referred to in paragraph 7 of any subsequently detected vu
58 items found		

DRAFT

3.3 EU-CRA compliance

The following table shows the compliance to the EU Cyber Resilence Act (EU 2024-2847 - final version, November 20th 2024)

Two aspect of the requirements are not considered in this version of the specifications: conformity assessment and EC declaration. Work is ongoing to define these two aspects for the railway sector. A future version is planned to integrate these results.

EU CRA	Requirement	Implemented by
EU-CRA 06-01	(1) they meet the essential requirements set out in Part I of Annex I, provided that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, the necessary security updates have been installed , and	_ is implemented by: EU-CRA Annex I: Annex I - Part I - Essential Cybersecurity requirements
EU-CRA 06-02	(2) the processes put in place by the manufacturer comply with the essential requirements set out in Part II of Annex I.	_ is implemented by: EU-CRA Annex I-2: Annex I-2 Vulnerability Handling Requirements
EU-CRA 13-01	1. When placing a product with digital elements on the market, manufacturers shall ensure that it has been designed, developed and produced in accordance with the essential cybersecurity requirements set out in Part I of Annex I.	_ is implemented by: EU-CRA Annex I: Annex I - Part I - Essential Cybersecurity requirements
EU-CRA 13-02	2. For the purposes of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing security incidents and minimising their impacts, including in relation to the health and safety of users.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SR-2: Specification of threat model including information flow, trust boundaries, processes, data storages, interacting external entities, communication protocols, accessible physical ports, potential attack vectors, potential threats, mitigations, security-related issues, external dependencies. Review of threat model at least once a year.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-03	The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Part I, point (2), of Annex I, are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Part I, point (1), of Annex I and the vulnerability handling requirements set out in Part II of Annex I.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SR-2: Specification of threat model including information flow, trust boundaries, processes, data storages, interacting external entities, communication protocols, accessible physical ports, potential attack vectors, potential threats, mitigations, security-related issues, external dependencies. Review of threat model at least once a year.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-04	When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment referred to in paragraph 3 of this Article in the technical documentation required pursuant to Article 31 and Annex VII. For products with digital elements referred to in Article 12, which are also subject to other Union legal acts, the cybersecurity risk assessment may be part of the risk assessment required by those Union legal acts. Where certain essential cybersecurity requirements are not applicable to the product with digital elements, the manufacturer shall include a clear justification to that effect in that technical documentation.	_ is implemented by: EU-CRA 31: Technical documentation _ is implemented by: EU-CRA Annex VII-3: Risk assessment _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-5-12: <description of use cases which may lead to significant security risks, incl. foreseeable misuse, known product vulnerabilities and risks associated with legacy code, together with mitigation strategies to address these risks> _ is implemented by: SP-SEC-DocTempl-5-6: <list of threats addressed by the defense in depth strategy>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-05	For the purpose of complying with paragraph 1, manufacturers shall exercise due diligence when integrating components sourced from third parties so that those components do not compromise the cybersecurity of the product with digital elements, including when integrating components of free and open-source software that have not been made available on the market in the course of a commercial activity.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SM-10: Conformation to the requirements of this standard for third-party suppliers for specifically developed components and component which can have an impact on security. _ is implemented by: IEC 62443-4-1 SM-9: Identification and managing the security risks of all externally provided components used for product development.
EU-CRA 13-06	Manufacturers shall, upon identifying a vulnerability in a component, including in an open source-component, which is integrated in the product with digital elements report the vulnerability to the person or entity manufacturing or maintaining the component, and address and remediate the vulnerability in accordance with the vulnerability handling requirements set out in Part II of Annex I. Where manufacturers have developed a software or hardware modification to address the vulnerability in that component, they shall share the relevant code or documentation with the person or entity manufacturing or maintaining the component, where appropriate in a machine-readable format.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SR-2: Specification of threat model including information flow,

DRAFT

EU CRA	Requirement	Implemented by
		trust boundaries, processes, data storages, interacting external entities, communication protocols, accessible physical ports, potential attack vectors, potential threats, mitigations, security-related issues, external dependencies. Review of threat model at least once a year.
EU-CRA 13-07	The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-2: <contact point / web site> _ is implemented by: SP-SEC-DocTempl-5-12: <description of use cases which may lead to significant security risks, incl. foreseeable misuse, known product vulnerabilities and risks associated with legacy code, together with mitigation strategies to address these risks> _ is implemented by: SP-SEC-DocTempl-5-5: <description of the security features and capabilities and

DRAFT

EU CRA	Requirement	Implemented by
		their support for defense of depth strategy>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-08-01	Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential requirements set out in Part II of Annex I.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: EU-CRA Annex I-P2-5: Manufacturers of the products with digital elements shall put in place and enforce a policy on coordinated vulnerability disclosure. _ is implemented by: EU-CRA Annex III: Important Products with Digital Elements _ is implemented by: IEC 62443-4-1 DM-3: Analyzation of security-related issues including impact assessment, definition of severity (e.g. CVSS), identification of other affected products, identification of root causes and identification of related security issues. _ is implemented by: IEC 62443-4-1 DM-5: Inform product users about reportable security-related issues in a timely manner including issue description, vulnerability score, affected product versions and description of the resolution _ is implemented by: IEC 62443-4-1 DM-4: Reporting security-related issues based on the results of the impact assessment. Address each issue including one or more of: fixing the issues, creating a remediation plan, deferring the problem, not fixing the problem. Inform other process and third parties.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-08-02	Manufacturers shall determine the support period so that it reflects the length of time during which the product is expected to be in use, taking into account, in particular, reasonable user expectations, the nature of the product, including its intended purpose, as well as relevant Union law determining the lifetime of products with digital elements. When determining the support period, manufacturers may also take into account the support periods of products with digital elements offering a similar functionality placed on the market by other manufacturers, the availability of the operating environment, the support periods of integrated components that provide core functions and are sourced from third parties as well as relevant guidance provided by the dedicated administrative cooperation group (ADCO) established pursuant to Article 52(15) and the Commission. The matters to be taken into account in order to determine the support period shall be considered in a manner that ensures proportionality.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>
EU-CRA 13-08-03	Without prejudice to the second subparagraph, the support period shall be at least five years. Where the product with digital elements is expected to be in use for less than five years, the support period shall correspond to the expected use time.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-08-05	Manufacturers shall include the information that was taken into account to determine the support period of a product with digital elements in the technical documentation as set out in Annex VII.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>
EU-CRA 13-08-06	Manufacturers shall have appropriate policies and procedures, including coordinated vulnerability disclosure policies, referred to in Part II, point (5), of Annex I to process and remediate potential vulnerabilities in the product with digital elements reported from internal or external sources.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-3: <web site>
EU-CRA 13-09	Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer.	_ is implemented by: SP-SEC-Pgrm-13.3.3-3: The supplier 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

DRAFT

EU CRA	Requirement	Implemented by
		support period, whichever is longer.
EU-CRA 13-10	Where a manufacturer has placed subsequent substantially modified versions of a software product on the market, that manufacturer may ensure compliance with the essential cybersecurity requirement set out in Part II, point (2), of Annex I only for the version that it has last placed on the market, provided that the users of the versions that were previously placed on the market have access to the version last placed on the market free of charge and do not incur additional costs to adjust the hardware and software environment in which they use the original version of that product.	
EU-CRA 13-12-01	Before placing a product with digital elements on the market, manufacturers shall draw up the technical documentation as referred to in Article 31.	_ is implemented by: EU-CRA 31: Technical documentation _ is implemented by: EU-CRA Annex I-2: Annex I-2 Vulnerability Handling Requirements _ is implemented by: EU-CRA 32: Conformity assessment procedures _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG).

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-12-02	The manufacturer shall carry out the chosen conformity assessment procedures as referred to in Article 32 or have them carried out.	
EU-CRA 13-12-03	Where compliance of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I has been demonstrated by that conformity assessment procedure, manufacturers shall draw up the EU declaration of conformity in accordance with Article 28 and affix the CE marking in accordance with Article 30.	
EU-CRA 13-13	Manufacturers shall keep the technical documentation and the EU declaration of conformity at the disposal of the market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.	_ is implemented by: 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 Secure 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

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-14	Manufacturers shall ensure that procedures are in place for products with digital elements that are part of a series of production to remain in conformity with this Regulation. Manufacturers shall adequately take into account changes in the development and production process or in the design or characteristics of the product with digital elements and changes in the harmonised standards, European cybersecurity certification schemes or common specifications as referred to in Article 27 by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SM-13: Improving continuously the security development lifecycle including defects analysis from field installed products. _ is implemented by: IEC 62443-4-1 SM-12: Verification of all security-related processes have been completed and documented _ is implemented by: IEC 62443-4-1 SM-1: Documentation and enforcement of a generic development/maintenance/support process including configuration management, requirement traceability, design and implementation practices, testing and validation process, review and approval process, life-cycle support

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-15	Manufacturers shall ensure that their products with digital elements bear a type, batch or serial number or other element allowing their identification, or, where that is not possible, that that information is provided on their packaging or in a document accompanying the product with digital elements.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-5: <description of how the product can be identified, e.g. locations of identifiers on labels on the product and via querying the diagnostic interface> _ is implemented by: SP-SEC-DocTempl-1-4: <serial number or batch number> _ is implemented by: SP-SEC-DocTempl-1-2: <Product Type> _ is implemented by: SP-SEC-Comp-5.2.8-1: The Secure Component shall bear a type, batch or serial number on its enclosure.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-16	Manufacturers shall indicate the name, registered trade name or registered trademark of the manufacturer, and the postal address, email address or other digital contact details, as well as, where applicable, the website where the manufacturer can be contacted, on the product with digital elements, on its packaging or in a document accompanying the product with digital elements. That information shall also be included in the information and instructions to the user set out in Annex II. The contact details shall be in a language which can be easily understood by users and market surveillance authorities.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-2-4: <email address or other digital contact> _ is implemented by: SP-SEC-DocTempl-2-5: <address to manufacturers contact page> _ is implemented by: SP-SEC-DocTempl-2-2: <Registered trade name or trade mark> _ is implemented by: SP-SEC-DocTempl-2-3: <Postal address> _ is implemented by: SP-SEC-DocTempl-2-1: <Manufacturer name> _ is implemented by: SP-SEC-DocTempl-0-2: 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.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-17	For the purposes of this Regulation, manufacturers shall designate a single point of contact to enable users to communicate directly and rapidly with them, including in order to facilitate reporting on vulnerabilities of the product with digital elements. Manufacturers shall ensure that the single point of contact is easily identifiable by the users. They shall also include the single point of contact in the information and instructions to the user set out in Annex II. The single point of contact shall allow users to choose their preferred means of communication and shall not limit such means to automated tools.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-2: <contact point / web site>

DRAFT

EU-CRA 13-18	Manufacturers shall ensure that products with digital elements are accompanied by the information and instructions to the user set out in Annex II, in paper or electronic form. Such information and instructions shall be provided in a language which can be easily understood by users and market surveillance authorities. They shall be clear, understandable, intelligible and legible. They shall allow for the secure installation, operation and use of products with digital elements. Manufacturers shall keep the information and instructions to the user set out in Annex II at the disposal of users and market surveillance authorities for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. Where such information and instructions are provided online, manufacturers shall ensure that they are accessible, user-friendly and available online for at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: EU-CRA Annex II: Information and Instructions to the User _ is implemented by: IEC 62443-4-1 SG-5: User documentation for secure operation and assumptions of users and administrator behavior. _ is implemented by: IEC 62443-4-1 SG-1: User documentation for the product user the security in depth strategy to support product installation, operation and maintenance including implemented security capabilities, addressed threats and user mitigation strategies for known security risks. _ is implemented by: SP-SEC-DocTempl-7-1: <detailed instruction on necessary measures during initial commissioning to ensure the secure use of the product> _ is implemented by: SP-SEC-DocTempl-9-1: <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> _ is implemented by: SP-SEC-DocTempl-10-1:

DRAFT

<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>

_ is implemented by: SP-SEC-DocTempl-7-2: <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 effects on security, how to set, change and delete the configuration value>

_ is implemented by: SP-SEC-DocTempl-8-1: <description of actions and responsibilities for user, including administrators>

_ is implemented by: 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 Secure 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

_ is implemented by: SP-SEC-DocTempl-0-2: 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.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-19	Manufacturers shall ensure that the end date of the support period referred to in paragraph 8, including at least the month and the year, is clearly and understandably specified at the time of purchase in an easily accessible manner and, where applicable, on the product with digital elements, its packaging or by digital means. Where technically feasible in light of the nature of the product with digital elements, manufacturers shall display a notification to users informing them that their product with digital elements has reached the end of its support period.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>
EU-CRA 13-20	Manufacturers shall either provide a copy of the EU declaration of conformity or a simplified EU declaration of conformity with the product with digital elements. Where a simplified EU declaration of conformity is provided, it shall contain the exact internet address at which the full EU declaration of conformity can be accessed.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-6: <web address to EU declaration of conformity for this product>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-21	From the placing on the market and for the support period, manufacturers who know or have reason to believe that the product with digital elements or the processes put in place by the manufacturer are not in conformity with the essential cybersecurity requirements set out in Annex I shall immediately take the corrective measures necessary to bring that product with digital elements or the manufacturer's processes into conformity, to withdraw or to recall the product, as appropriate.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SUM-4: Make available security updates for all supported products and product versions to product users including verification of patch authenticity.
EU-CRA 13-22	Manufacturers shall, upon a reasoned request from a market surveillance authority, provide that authority, in a language which can be easily understood by that authority, with all the information and documentation, in paper or electronic form, necessary to demonstrate the conformity of the product with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Annex I. Manufacturers shall cooperate with that authority, at its request, on any measures taken to eliminate the cybersecurity risks posed by the product with digital elements which they have placed on the market.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 13-23	A manufacturer that ceases its operations and, as a result, is not able to comply with this Regulation shall inform, before the cessation of operations takes effect, the relevant market surveillance authorities as well as, by any means available and to the extent possible, the users of the relevant products with digital elements placed on the market, of the impending cessation of operations.	_ is implemented by: SP-SEC-Pgrm-13.3.3-4: If a supplier ceases its operation, the supplier shall inform the relevant market authorities and the users of the affected products about this situation.

DRAFT

EU-CRA 14-01	A manufacturer shall notify any actively exploited vulnerability contained in the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify t hat actively exploited vulnerability via the single reporting platform established pursuant to article 16.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 DM-1: Receive and track to closure security-related issues reported by internal and external sources including (security testers, suppliers, product developers, product users) _ is implemented by: IEC 62443-4-1 DM-2: Investigation of security-related issues in a timely manner including determination of applicability, verifiability and threats trigger the issue _ is implemented by: IEC 62443-4-1 DM-3: Analyzation of security-related issues including impact assessment, definition of severity (e.g. CVSS), identification of other affected products, identification of root causes and identification of related security issues. _ is implemented by: IEC 62443-4-1 DM-5: Inform product users about reportable security-related issues in a timely manner including issue description, vulnerability score, affected product versions and description of the resolution _ is implemented by: IEC 62443-4-1 DM-4: Reporting security-related issues based on the results of the impact assessment. Address each issue including one or more of: fixing the issues, creating a remediation plan, deferring the problem, not fixing the problem. Inform other process and third parties.

DRAFT

EU-CRA 14-02	For the purposes of the notification referred to in paragraph 1, the manufacturer shall submit: (a) an early warning notification of an actively exploited vulnerability, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, indicating, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available; (b) unless the relevant information has already been provided, a vulnerability notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the actively exploited vulnerability, which shall provide general information, as available, about the product with digital elements concerned, the general nature of the exploit and of the vulnerability concerned as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be; (c) unless the relevant information has already been provided, a final report, no later than 14 days after a corrective or mitigating measure is available, including at least the following: (i) a description of the vulnerability, including its severity and impact; (ii) where available, information concerning any malicious actor that has exploited or that is exploiting the vulnerability; (iii) details about the security update or other corrective measures that have been made available to remedy the vulnerability.	_ is implemented by: SP-SEC-Pgrm-13.3.1-1: The supplier shall submit an early warning notification to the designated CSIRT, ENISA and to affected customers of actively exploited 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. _ is implemented by: SP-SEC-Pgrm-13.3.1-3: The supplier shall submit a vulnerability information to the designated CSIRT, ENISA and affected customers of actively exploited vulnerabilities in Secure Components with undue delay and within of 72h of becoming aware of it. _ is implemented by: SP-SEC-Pgrm-13.3.1-4: The supplier shall submit a final report to the designated CSIRT 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.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 14-03	A manufacturer shall notify any severe incident having an impact on the security of the product with digital elements that it becomes aware of simultaneously to the CSIRT designated as coordinator, in accordance with paragraph 7 of this Article, and to ENISA. The manufacturer shall notify that incident via the single reporting platform established pursuant to Article 16.	_ is implemented by: SP-SEC-Pgrm-13.3.2-1: The supplier shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at supplier 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 supplier. 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

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 14-04	For the purposes of the notification referred to in paragraph 3, the manufacturer shall submit: (a) an early warning notification of a severe incident having an impact on the security of the product with digital elements, without undue delay and in any event within 24 hours of the manufacturer becoming aware of it, including at least whether the incident is suspected of being caused by unlawful or malicious acts, which shall also indicate, where applicable, the Member States on the territory of which the manufacturer is aware that their product with digital elements has been made available; (b) unless the relevant information has already been provided, an incident notification, without undue delay and in any event within 72 hours of the manufacturer becoming aware of the incident, which shall provide general information, where available, about the nature of the incident, an initial assessment of the incident, as well as any corrective or mitigating measures taken, and corrective or mitigating measures that users can take, and which shall also indicate, where applicable, how sensitive the manufacturer considers the notified information to be; (c) unless the relevant information has already been provided, a final report, within one month after the submission of the incident notification under point (b), including at least the following: (i) a detailed description of the incident, including its severity and impact; (ii) the type of threat or root cause that is likely to have triggered the incident; (iii) applied and ongoing mitigation measures.	_ is implemented by: SP-SEC-Pgrm-13.3.2-1: The supplier shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any severe incident at supplier 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 supplier. 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 _ is implemented by: SP-SEC-Pgrm-13.3.2-2: The supplier shall submit an incident notification within 72h to the designated CSIRT and to ENISA of any severe incident at supplier 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. _ is implemented by: SP-SEC-Pgrm-13.3.2-3: The supplier shall submit a final report within one month to the designated CSIRT and to ENISA of any severe incident at supplier 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.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 14-08	After becoming aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product with digital elements, the manufacturer shall inform the impacted users of the product with digital elements, and where appropriate all users, of that vulnerability or incident and, where necessary, of any risk mitigation and corrective measures that the users can deploy to mitigate the impact of that vulnerability or incident, where appropriate in a structured, machine-readable format that is easily automatically processable,. Where the manufacturer fails to inform the users of the product with digital elements in a timely manner, the notified CSIRTs designated as coordinators may provide such information to the users when considered to be proportionate and necessary for preventing or mitigating the impact of that vulnerability or incident.	_ is implemented by: SP-SEC-Pgrm-13.3.2-4: The supplier 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. _ is implemented by: SP-SEC-Pgrm-13.3.1-3: The supplier shall submit a vulnerability information to the designated CSIRT, ENISA and affected customers of actively exploited vulnerabilities in Secure Components with undue delay and within of 72h of becoming aware of it.
EU-CRA 31-01	The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential cybersecurity requirements set out in Annex I. It shall at least contain the elements set out in Annex VII.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG).

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 31-02	The technical documentation shall be drawn up before the product with digital elements is placed on the market and shall be continuously updated, where appropriate, at least during the support period	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SM-13: Improving continuously the security development lifecycle including defects analysis from field installed products. _ is implemented by: IEC 62443-4-1 SG-7: Identification and track to closure of errors and omissions of all user manuals. _ is implemented by: SP-SEC-Comp-6.3-3: The manufacturer shall update continuously the Secure Component technical documentation, where appropriate, for at least during the support period.
EU-CRA 31-04	The technical documentation and correspondence relating to any conformity assessment procedure shall be drawn up in an official language of the Member State in which the notified body is established or in a language acceptable to that body.	_ is implemented by: SP-SEC-Comp-6.3-2: The Secure Component documentation shall be written in an official language of the EU member states in a clear, understandable, intelligible and legible manner.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 32-01	The manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential cybersecurity requirements set out in Annex I are met. The manufacturer shall demonstrate conformity with the essential cybersecurity requirements by using any of the following procedures: (a) the internal control procedure (based on module A) set out in Annex VIII; (b) the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; (c) conformity assessment based on full quality assurance (based on module H) set out in Annex VIII; or (d) where available and applicable, a European cybersecurity certification scheme as specified in Article 27(9).	
EU-CRA 32-02	Where, in assessing the compliance of an important product with digital elements that falls under class I as set out in Annex III and the processes put in place by its manufacturer with the essential cybersecurity requirements set out in Annex I, the manufacturer has not applied or has applied only in part harmonised standards, common specifications or European cybersecurity certification schemes at assurance level at least ‘substantial’ as referred to in Article 27, or where such harmonised standards, common specifications or European cybersecurity certification schemes do not exist, the product with digital elements concerned and the processes put in place by the manufacturer shall be submitted with regard to those essential cybersecurity requirements to any of the following procedures:	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA 32-02a	the EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII; or	
EU-CRA 32-02b	a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII.	
EU-CRA 32-03a	EU-type examination procedure (based on module B) set out in Annex VIII followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VIII	
EU-CRA 32-03b	a conformity assessment based on full quality assurance (based on module H) set out in Annex VIII	
EU-CRA 32-03c	where available and applicable, a European cybersecurity certification scheme pursuant to Article 27(9) of this Regulation at assurance level at least ‘substantial’ pursuant to Regulation (EU) 2019/881.	
EU-CRA 32-3	Where the product is an important product with digital elements that falls under class II as set out in Annex III, the manufacturer shall demonstrate conformity with the essential cybersecurity requirements set out in Annex I by using any of the following procedures:	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-1	(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SR-4: Definition of scope and boundaries of the component or system (physical and logical) and required capability security level (SL-C) of the product. _ is implemented by: IEC 62443-4-1 SR-2: Specification of threat model including information flow, trust boundaries, processes, data storages, interacting external entities, communication protocols, accessible physical ports, potential attack vectors, potential threats, mitigations, security-related issues, external dependencies. Review of threat model at least once a year.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2a	Products with digital elements shall shall be made available on the market without any known exploitable vulnerabilities;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SVV-3: Perform tests focusing on security vulnerabilities including abuse case or malformed tests (e.g. fuzz testing, network load tests, attack surface analysis, black box vulnerability scanning, software composition analysis, dynamic runtime resource management testing.
EU-CRA Annex I-P1-2b	Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state.	_ is implemented by: SP-SEC-Serv-12.5-1: The SSI-MNT interface shall provide the maintenance method SS `I-MNT:ComponentLifecycleManagement:InitiateFactoryReset()`, which deletes persistent data to reset the component to factory state. Note 1: this method can be used as part of a decommissioning process Note 2: this method does not delete the factory key material (e.g. the MDC together with its root certificate will stay on the devices). Note 3: this methods provides the user with the ability to erase data which requires confidentiality protection from persistent memory. _ is implemented by: SP-SEC-Comp-6.2-3: The Secure Component shall have a factory configuration that is secure by default.

DRAFT

EU CRA	Requirement	Implemented by
		Note: a secure by default configuration is a configuration that has all configurable security functions enabled.
EU-CRA Annex I-P1-2c	Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them.	_ is implemented by: SP-SEC-Comp-5.6.1-1: The Secure Component shall support the update of software and configuration via the interface [I-STD-MAINTENANCE - SMI] . Note 1: when updating non-safety related software, typically also the process allowlist has to be updated. Note 2: this supports together with the backup and restore functionality (chapter 5.6.3) the recovery and reconstitution to a known secure state after a disruption or failure.

DRAFT

EU-CRA Annex I-P1-2d	Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access.	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-CommExt-1.4-4: Each software process realizing an additional communication interface shall enforce access based on retrieved permissions. Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. _ is implemented by: SP-SEC-Comp-7.1.1-9: The Network Component shall support authentication on all enabled management network interfaces. _ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other

DRAFT

identification schemes are applicable.

_ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events:

a) access control;

b) request errors;

c) control system events;

d) backup and restore event;

e) configuration changes; and

f) audit log events (incl. administrative actions, input validation errors)

g) threats (attacks and probes)

h) resource events (system resources reaching a threshold)

i) availability (shutdown, failures, crashes).

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2e	Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means.	_ is implemented by: SP-SEC-Comp-5.3.3-1: If read access authorisation to persistent data is required, the Secure Component shall encrypt this data. Note: this applies at least for all confidential data at rest. It could be realized using file system encryption which encrypts all persistent data. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec]. _ is implemented by: SP-SEC-Comp-7.1.1-10: The Network Component shall support integrity and encryption protection for the protocols used for the enabled management network interfaces. _ is implemented by: SP-SEC-CommExt-1.5-2: If data in transit is considered confidential, a software process realizing an additional communication interface shall provide the capability to protect the confidentiality of data in transit. Note: this should, if applicable, be realized preferable using TLS with an encryption cipher. Examples of confidential data in transit are encryption keys, legally protected personal data, user credentials, person/user related data, financial information, security related logs and/or diagnosis data.

DRAFT

EU-CRA Annex I-P1-2f	Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;	_ is implemented by: SP-SEC-Comp-5.3.2-1: The Secure Component shall verify the integrity and authenticity of configuration data using the installed roots of trust before it is used. Note: configuration data is cryptographically signed. Verification of integrity and authenticity is done by verifying the signature. _ is implemented by: SP-SEC-Comp-5.2.5-4: If an integrity check of a secure boot stage fails during secure boot, the Secure Component shall terminate the boot process. _ is implemented by: SP-SEC-CommExt-1.5-1: Each software process realizing an additional communication interface shall protect the integrity of data in transit. Note: this should, if applicable, be realized preferable using TLS with an integrity cipher. In any case, a cryptographic method for integrity protection is required _ is implemented by: SP-SEC-Comp-5.3.2-2: For retrieval of log data, the Secure Component shall protect the integrity of log data by restricting authorised users to read-only access. Note: For writing to log, applications/software processes typically use a logging API to append data to the log. The log is generally protected by the operating system, e.g. applications/software processes have no direct access to the log (see also hardening requirements). External users (human or technical users) have read-only access. _ is implemented by: SP-SEC-Comp-5.3.2-3: If a Secure Component is implementing a Juridical Recording function, then it shall protect the integrity of

DRAFT

juridical recording data at rest.

Note: If personal identifiable information or financial data is recorded, as of GDPR also confidentiality needs to be considered

_ is implemented by: SP-SEC-Comp-5.6.2-2: The update package shall use SHA-512 hash algorithm for the integrity protection.

_ is implemented by: SP-SEC-Comp-5.3.1-1: The Secure Component shall only start a software process if it passes the runtime integrity check.

Note: This protects against execution of unauthorised software. Typical solutions are a process allowlist or anomaly detection. An allowlist typically contains the hashes of the authorised executable binaries.

_ is implemented by: SP-SEC-Comp-5.2.3-2: The Secure Component shall protect the integrity of roots of trust (root certificates) via a commonly accepted cryptographic mechanism originating from hardware.

Note: examples of commonly accepted cryptographic mechanism originating from hardware are trusted execution environment (TEE), trusted platform module (TPM 2.0 or higher), hardware security module (HSM).

_ is implemented by: SP-SEC-Comp-5.3.1-2: At startup, the Secure Component shall check the integrity and authenticity of runtime integrity check.

Note: if the process runtime-integrity check is realised using an process allowlist, this could be part of the firmware and therefore is part of the secure boot process. If the allowlist is outside of the secure boot process (e.g. on a configuration partition), a possible solution is the signing of the allowlist with the certificate of the software manufacturer.

_ is implemented by: SP-SEC-Comp-5.2.5-5: The

DRAFT

		Secure Component shall continue with the next boot stage only if the integrity and authenticity checks are successful. _ is implemented by: SP-SEC-Comp-5.6.3-3: If the Secure Component backups operational data, the Secure Component shall be capable of verifying the authenticity and integrity of backup data received via SSI-BKP SP-SEC-ServSpec Ch 11 - BKP: Backup and Restore _ is implemented by: SP-SEC-Comp-7.1.1-10: The Network Component shall support integrity and encryption protection for the protocols used for the enabled management network interfaces.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2g	Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (‘data minimisation’).	_ is implemented by: SP-SEC-Comp-5.4.5-1: The Secure Component shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the Secure Component (‘data minimisation’).
EU-CRA Annex I-P1-2h	Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial of service attacks.	_ is implemented by: SP-SEC-Comp-5.4.4-2: After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally. Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds. This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1 _ is implemented by: SP-SEC-Comp-5.4.4-1: The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion. Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits. _ is implemented by: SP-SEC-CommExt-1.7-1: DoS resilience for communication interfaces is required by EU CRA and IEC 62443-4-2. Corresponding requirements can be found in SP-SEC-CompSpec-5.4.4 Denial of service resilience

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2i	Products with digital elements shall minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks.	_ is implemented by: SP-SEC-Comp-5.4.2-3: The Secure Component's host-based firewall filter shall be capable of filtering incoming and outgoing network traffic. _ is implemented by: SP-SEC-Comp-5.3.6-1: The Secure Component shall enable only required and documented functions and services and their corresponding exposed ports and protocols. Note: Examples for possible unused functions and services are email, voice over IP, instant messaging, and file transfer protocol (FTP). This requirement can be verfied by external port scans (no difference between documented required ports and detected ports). When using standard OS and applications, OS and application hardenening can be an essential measure to fulfill this requirement. Hardening can be demonstrated by a relevant **[CIS benchmark]**, achieving compliance to at least Level 1 or in accordance with a comparable benchmark and compliance level. _ is implemented by: SP-SEC-Comp-5.4.2-2: The host-based firewall shall deny by default all inbound and outbound connections except for the designed network communications of the Secure Component. _ is implemented by: SP-SEC-Comp-5.4.2-1: The Secure Component shall provide the capability of a host-based firewall (e.g. packet filter using IP addresses, destination and source port, protocol and connection state (TCP) as filter parameter). _ is implemented by: SP-SEC-CommExt-1.7-2: Minimising negative impact to network and to connected devices is required by EU CRA. Corresponding requirements can be found in SP-SEC-CompSpec-5.4.2 Host-based firewall

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2j	Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces.	_ is implemented by: SP-SEC-Comp-5.3.6-1: The Secure Component shall enable only required and documented functions and services and their corresponding exposed ports and protocols. Note: Examples for possible unused functions and services are email, voice over IP, instant messaging, and file transfer protocol (FTP). This requirement can be verfied by external port scans (no difference between documented required ports and detected ports). When using standard OS and applications, OS and application hardenening can be an essential measure to fulfill this requirement. Hardening can be demonstrated by a relevant **[CIS benchmark]**, achieving compliance to at least Level 1 or in accordance with a comparable benchmark and compliance level.
EU-CRA Annex I-P1-2k	Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SD-2: Implementation of multiple layers of defense and assigning responsibilities to each layer.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2l	Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user.	_ is implemented by: SP-SEC-CommExt-1.6-1: Security logging for communication interface accesses is required by EU CRA and IEC 62443-4-2. Corresponding requirements can be found in SP-SEC-CompSpec-5.7 - Logging and Diagnostic _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P1-2m	Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-10-1: <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>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P2-1	Manufacturers of the products with digital elements shall identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 DM-1: Receive and track to closure security-related issues reported by internal and external sources including (security testers, suppliers, product developers, product users) _ is implemented by: 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..

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P2-2	Manufacturers of the products with digital elements shall in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SUM-4: Make available security updates for all supported products and product versions to product users including verification of patch authenticity. _ is implemented by: IEC 62443-4-1 DM-4: Reporting security-related issues based on the results of the impact assessment. Address each issue including one or more of: fixing the issues, creating a remediation plan, deferring the problem, not fixing the problem. Inform other process and third parties.
EU-CRA Annex I-P2-3	Manufacturers of the products with digital elements shall apply effective and regular tests and reviews of the security of the product with digital elements;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SVV-1:

DRAFT

EU CRA	Requirement	Implemented by
		Verification of product security functions meeting the security requirements including functional testing of security requirements, performance and scalability testing and boundary/edge condition, stress and malformed input test.
EU-CRA Annex I-P2-4	Manufacturers of the products with digital elements shall once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SUM-4: Make available security updates for all supported products and product versions to product users including verification of patch authenticity. _ is implemented by: IEC 62443-4-1 DM-5: Inform product users about reportable security-related issues in a timely manner including issue description, vulnerability score, affected product versions and description of the resolution

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P2-5	Manufacturers of the products with digital elements shall put in place and enforce a policy on coordinated vulnerability disclosure.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-3: <web site>
EU-CRA Annex I-P2-6	Manufacturers of the products with digital elements shall take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-1: <contact point / web site>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P2-7	Manufacturers of the products with digital elements shall provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: SP-SEC-Comp-5.6.1-3: The Secure Component shall verify the signature of the update packages using the corresponding installed roots of trust before installation. _ is implemented by: SP-SEC-Comp-5.6.2-1: The update package shall be signed using the corresponding update signing key. Note: the corresponding update signing key for firmware update is the MUSC and for configuration update is the MCSC or OCSC. _ is implemented by: IEC 62443-4-1 SUM-5: Delivering and qualifying security updates in specified timeframes to product users including potential impact of the vulnerability, public vulnerability knowledge, existence of exploits, volume of affected products, availability of an effective mitigation. _ is implemented by: SP-SEC-Pgrm-13.3.3-1: The supplier shall provide for mechanisms to securely distribute updates for Secure Components (e.g. using the updated package defined in SP-SEC-CompSpec Ch

DRAFT

EU CRA	Requirement	Implemented by
		5.6.2 - Update package).

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex I-P2-8	Manufacturers of the products with digital elements shall ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SUM-5: Delivering and qualifying security updates in specified timeframes to product users including potential impact of the vulnerability, public vulnerability knowledge, existence of exploits, volume of affected products, availability of an effective mitigation. _ is implemented by: SP-SEC-Pgrm-13.3.3-2: The supplier shall provide the security patches or updates without undue delay accompanied by advisory messages providing users with the relevant information, including on potential actions to be taken.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-1	1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-5: <description of how the product can be identified, e.g. locations of identifiers on labels on the product and via querying the diagnostic interface> _ is implemented by: SP-SEC-DocTempl-2-4: <email address or other digital contact> _ is implemented by: SP-SEC-DocTempl-2-5: <address to manufacturers contact page> _ is implemented by: SP-SEC-DocTempl-2-2: <Registered trade name or trade mark> _ is implemented by: SP-SEC-DocTempl-2-3: <Postal address> _ is implemented by: SP-SEC-DocTempl-2-1: <Manufacturer name> _ is implemented by: SP-SEC-DocTempl-1-4: <serial number or batch number>
EU-CRA Annex II-2	2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product.

DRAFT

EU CRA	Requirement	Implemented by
		Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-1: <contact point / web site> _ is implemented by: SP-SEC-DocTempl-3-3: <web site> _ is implemented by: SP-SEC-DocTempl-3-2: <contact point / web site>
EU-CRA Annex II-3	3. name and type and any additional information enabling the unique identification of the product with digital elements;	_ is implemented by: SP-SEC-Comp-5.2.7-2: The security seal shall contain a number unique to the supplier. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-2: <Product Type> _ is implemented by: SP-SEC-DocTempl-1-1: <Product Name> _ is implemented by: SP-SEC-DocTempl-1-3: <Product Version>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-4	4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SG-2: User documentation for security defense in depth measures expected by the external environment. _ is implemented by: IEC 62443-4-1 SG-1: User documentation for the product user the security in depth strategy to support product installation, operation and maintenance including implemented security capabilities, addressed threats and user mitigation strategies for known security risks. _ is implemented by: SP-SEC-DocTempl-4-2: <description of the implemented essential functions and supported essential functions> _ is implemented by: SP-SEC-DocTempl-5-1: <degree of compliance to referred security standards> _ is implemented by: SP-SEC-DocTempl-4-1: <description of main features and intended usage> _ is implemented by: SP-SEC-DocTempl-5-10: <description of the provided security environment>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-5	5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SG-5: User documentation for secure operation and assumptions of users and administrator behavior. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-5-12: <description of use cases which may lead to significant security risks, incl. foreseeable misuse, known product vulnerabilities and risks associated with legacy code, together with mitigation strategies to address these risks>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-6	6. where applicable, the internet address at which the EU declaration of conformity can be accessed;	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-6: <web address to EU declaration of conformity for this product>
EU-CRA Annex II-7	7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years> _ is implemented by: SP-SEC-DocTempl-5-13: <description which type of security support is offered for this product>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-8	9. detailed instructions or an internet address referring to such detailed instructions and information on:	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-7-1: <detailed instruction on necessary measures during initial commissioning to ensure the secure use of the product> _ is implemented by: SP-SEC-DocTempl-9-1: <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>

DRAFT

EU-CRA Annex II-8a	(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SG-1: User documentation for the product user the security in depth strategy to support product installation, operation and maintenance including implemented security capabilities, addressed threats and user mitigation strategies for known security risks. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-7-1: <detailed instruction on necessary measures during initial commissioning to ensure the secure use of the product> _ is implemented by: SP-SEC-DocTempl-9-1: <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

DRAFT

		procedures, verification of successful backup, backup and restore related audit logs and restoration steps supporting disaster recovery>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-8b	(b) how changes to the product with digital elements can affect the security of data;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SG-1: User documentation for the product user the security in depth strategy to support product installation, operation and maintenance including implemented security capabilities, addressed threats and user mitigation strategies for known security risks. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-5-14: <description which changes can affect the security of the products>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-8c	(c) how security-relevant updates can be installed;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SUM-2: Documentation of product security updates including product version, application instruction, verification instructions, risk of not applying patch. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-9-3: <description how to verify authenticity and integrity of updates and how to install updates, including if a restart of the product is required>

DRAFT

EU-CRA Annex II-8d	(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SG-4: User documentation for removing product from use including removing references and configuration data in the environment, secure removal of data stored in the product, secure disposal of product. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-10-1: <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>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-8e	how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-9-4: <description how automatic security update function is disabled>
EU-CRA Annex II-8f	where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-5-11: <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, including physical security requirements>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex II-9	If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-7: <if made available, web address of software bill of material in CycloneDX SBOM standard format of this product>
EU-CRA Annex III	No requirements in this section. The section contains the list of class 1 and class 2 important products with digital elements.	
EU-CRA Annex IV	No requirements in this section. The section contains the list of critical products with digital elements.	
EU-CRA Annex V	The section contains the requirements for EU Declaration of Conformity (conformity is not considered in this version of the specification)	
EU-CRA Annex VI	The section contains requirements for Simplified EU Declaration of Conformity (conformity is not considered in this version of the specification)	
EU-CRA Annex VII-1	1. a general description of the product with digital elements, including:	
EU-CRA Annex VII-1a	(a) its intended purpose;	
EU-CRA Annex VII-1b	(b) versions of software affecting compliance with essential cybersecurity requirements;	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VII-1c	(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;	
EU-CRA Annex VII-1d	(d) user information and instructions as set out in Annex II;	_ is implemented by: EU-CRA Annex VII-2c: (c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes.
EU-CRA Annex VII-2	2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security)
EU-CRA Annex VII-2a	(a) necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;	_ is implemented by: SP-SEC-Comp-6.2-3: The Secure Component shall have a factory configuration that is secure by default. Note: a secure by default configuration is a configuration that has all configurable security functions enabled. _ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product.

DRAFT

EU CRA	Requirement	Implemented by
		Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG).
EU-CRA Annex VII-2b	(b) necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;	
EU-CRA Annex VII-2c	(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VII-3	3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SR-2: Specification of threat model including information flow, trust boundaries, processes, data storages, interacting external entities, communication protocols, accessible physical ports, potential attack vectors, potential threats, mitigations, security-related issues, external dependencies. Review of threat model at least once a year.
EU-CRA Annex VII-4	4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;	_ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VII-5	5. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in of Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security)
EU-CRA Annex VII-6	6.reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) _ is implemented by: IEC 62443-4-1 SVV-1: Verification of product security functions meeting the security requirements including functional testing of security requirements, performance and scalability testing and boundary/edge condition, stress and malformed input test.

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VII-7	7. a copy of the EU declaration of conformity;	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-6: <web address to EU declaration of conformity for this product>
EU-CRA Annex VII-8	8. where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). _ is implemented by: SP-SEC-DocTempl-1-7: <if made available, web address of software bill of material in CycloneDX SBOM standard format of this product>
EU-CRA Annex VIII-P1-2	The manufacturer shall draw up the technical documentation described in Annex VII.	_ is implemented by: SP-SEC-Comp-6.3-1: The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product. Note: Such a file format may be for example PDF-A, Office Open

DRAFT

EU CRA	Requirement	Implemented by
		XML, Drawing Interchange Format, Scalable Vector Graphics (SVG).
EU-CRA Annex VIII-P1-3	The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Parts I and II of Annex I.	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security)
EU-CRA Annex VIII-P1-4.1	The manufacturer shall affix the CE marking to each individual product with digital elements that satisfies the applicable requirements set out in this Regulation	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P1-4.2	The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 28 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.	_ is implemented by: SP-SEC-DocTempl-1-6: <web address to EU declaration of conformity for this product>
EU-CRA Annex VIII-P1-5	The manufacturer’s obligations set out in point 4 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.	
EU-CRA Annex VIII-P2-01	1. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.	
EU-CRA Annex VIII-P2-02	2. EU-type examination shall be carried out by assessment of the adequacy of the technical design and development of the product with digital elements through examination of the technical documentation and supporting evidence referred to in point 3, plus examination of specimens of one or more critical parts of the product (combination of production type and design type).	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P2-03	3. The manufacturer shall lodge an application for EU-type examination with a single notified body of its choice.	
EU-CRA Annex VIII-P2-03.1	The application shall include the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;	
EU-CRA Annex VIII-P2-03.2	The application shall include a written declaration that the same application has not been lodged with any other notified body;	
EU-CRA Annex VIII-P2-03.3	The application shall include the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Annex I, Part I, and the manufacturer's vulnerability handling processes set out in Part II of Annex I, and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;	
EU-CRA Annex VIII-P2-03.4	The application shall include the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on his behalf and under its responsibility.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P2-04.1	The notified body shall examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I, and of the vulnerability handling processes put in place by the manufacturer with the essential requirements set out in Part II of Annex I;	
EU-CRA Annex VIII-P2-04.2	The notified body shall verify that specimens have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;	
EU-CRA Annex VIII-P2-04.3	The notified body shall carry out appropriate examinations and tests, or have them carried out, to check that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I, these have been applied correctly;	
EU-CRA Annex VIII-P2-04.4	The notified body shall carry out appropriate examinations and tests, or have them carried out, to check that, where the solutions in the relevant harmonised standards or technical specifications for the cybersecurity requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential requirements;	
EU-CRA Annex VIII-P2-04.5	The notified body shall agree with the manufacturer on a location where the examinations and tests will be carried out.	
EU-CRA Annex VIII-P2-05	The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P2-06	Where the type and the vulnerability handling processes meet the essential cybersecurity requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached. The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with digital elements with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control. Where the type and the vulnerability handling processes do not satisfy the applicable essential cybersecurity requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P2-07	The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential cybersecurity requirements set out in Annex I to this Regulation, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly. The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.	
EU-CRA Annex VIII-P2-08	The notified body shall carry out periodic audits to ensure that the vulnerability handling processes as set out in Part II of Annex I, are implemented adequately	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P2-09	Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and/or any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and any additions thereto refused, suspended or otherwise restricted. Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and additions thereto which it has issued. The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and any additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.	
EU-CRA Annex VIII-P2-10	9. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.	
EU-CRA Annex VIII-P2-11	10. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 10, provided that the relevant obligations are specified in the mandate.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P3-3.1	The manufacturer shall affix the CE marking to each individual product with digital elements that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements set out in the legislative instrument.	
EU-CRA Annex VIII-P3-3.2	The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	
EU-CRA Annex VIII-P3-4	The manufacturer's obligations set out in point 3 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.	
EU-CRA Annex VIII-P4-1	Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 5 of this Part, and ensures and declares on its sole responsibility that the products with digital elements or product categories concerned satisfy the essential cybersecurity requirements set out in Part I of Annex I, and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Part II of Annex I.	
EU-CRA Annex VIII-P4-2	The manufacturer shall operate an approved quality system as specified in point 3 for the design, development and final product inspection and testing of the products with digital elements concerned and for handling vulnerabilities, maintain its effectiveness throughout the support period, and shall be subject to surveillance as specified in point 4.	
EU-CRA Annex VIII-P4-3.1	The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-3.1a	The application shall include the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;	
EU-CRA Annex VIII-P4-3.1b	The application shall includethe technical documentation for one model of each category of products with digital elements intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex VII;	
EU-CRA Annex VIII-P4-3.1c	The application shall include the documentation concerning the quality system	
EU-CRA Annex VIII-P4-3.1d	The application shall include a written declaration that the same application has not been lodged with any other notified body.	
EU-CRA Annex VIII-P4-3.2	The quality system shall ensure compliance of the products with digital elements with the essential cybersecurity requirements set out in Part I of Annex I, and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Part II of Annex I. All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records. It shall, in particular, contain an adequate description of:	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-3.2a	– the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;	
EU-CRA Annex VIII-P4-3.2b	– the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part I of Annex I, that apply to the products with digital elements will be met;	
EU-CRA Annex VIII-P4-3.2c	– the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part II of Annex I, that apply to the manufacturer will be met;	
EU-CRA Annex VIII-P4-3.2d	– the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products pertaining to the product category covered;	
EU-CRA Annex VIII-P4-3.2e	– the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;	
EU-CRA Annex VIII-P4-3.2f	– the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;	
EU-CRA Annex VIII-P4-3.2g	– the quality records, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned;	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-3.2h	– the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.	
EU-CRA Annex VIII-P4-3.3	3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2. It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard and/or technical specification. In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and shall have knowledge of the applicable requirements set out in this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1 (b), to verify the manufacturer's ability to identify the applicable requirements of this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with digital elements with those requirements. The manufacturer or its authorised representative shall be notified of the decision. The notification shall contain the conclusions of the audit and the reasoned assessment decision.	
EU-CRA Annex VIII-P4-3.4	The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-3.5	The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system. The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary. It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.	
EU-CRA Annex VIII-P4-3.5	The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system. 3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system. The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point	
EU-CRA Annex VIII-P4-4.1	The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.	
EU-CRA Annex VIII-P4-4.2	The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-4.2a	– the quality system documentation;	
EU-CRA Annex VIII-P4-4.2b	– the quality records as provided for by the design part of the quality system, such as results of analyses, calculations and tests;	
EU-CRA Annex VIII-P4-4.2c	– the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned.	
EU-CRA Annex VIII-P4-4.3	The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.	
EU-CRA Annex VIII-P4-5.1	The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product with digital elements that satisfies the requirements set out in Part I of Annex I to this Regulation.	
EU-CRA Annex VIII-P4-5.2	The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up. A copy of the declaration of conformity shall be made available to the relevant authorities upon request.	

DRAFT

EU CRA	Requirement	Implemented by
EU-CRA Annex VIII-P4-6	The manufacturer shall, for a period ending at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep at the disposal of the national authorities:	
EU-CRA Annex VIII-P4-6.1	– the technical documentation referred to in point 3.1;	
EU-CRA Annex VIII-P4-6.2	– the documentation concerning the quality system referred to in point 3.1;	
EU-CRA Annex VIII-P4-6.3	– the change referred to in point 3.5, as approved;	
EU-CRA Annex VIII-P4-6.4	– the decisions and reports of the notified body referred to in points 3.5 and 4.3.	
EU-CRA Annex VIII-P4-8	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.	
163 items found		

DRAFT

3.4 EU-RED compliance

Table containing RED req no, title and corresponding req or chapter in this doc

EU RED	Requirement	Implemented by
EU-RED-1-1	The essential requirement set out in Article 3(3), point (d), of Directive 2014/53/EU shall apply to any radio equipment that can communicate itself over the internet, whether it communicates directly or via any other equipment ('internet-connected radio equipment').	_ is implemented by: EU-RED-3-3d: (d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.
EU-RED-1-2	The essential requirement set out in Article 3(3), point (e), of Directive 2014/53/EU shall apply to any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data and location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC: (a) internet-connected radio equipment, other than the equipment referred to in points (b), (c) or (d); (b) radio equipment designed or intended exclusively for childcare; (c) radio equipment covered by Directive 2009/48/EC; (d) radio equipment designed or intended, whether exclusively or not exclusively, to be worn on, strapped to, or hung from any of the following: (i) any part of the human body, including the head, neck, trunk, arms, hands, legs and feet; (ii) any clothing, including headwear, hand wear and footwear, which is worn by human beings.	_ is implemented by: EU-RED-3-3e: (e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
EU-RED-1-3	The essential requirement set out in Article 3(3), point (f), of Directive 2014/53/EU shall apply to any internet-connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713.	_ is implemented by: EU-RED-3-3f: (f): radio equipment supports certain features ensuring protection from fraud;

DRAFT

EU RED	Requirement	Implemented by
EU-RED-3-3d	(d): radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.	_ is implemented by: SP-SEC-COMM-3.1-3: The TLS endpoint shall enforce mutual authentication. _ is implemented by: SP-SEC-Comp-5.4.2-3: The Secure Component's host-based firewall filter shall be capable of filtering incoming and outgoing network traffic. _ is implemented by: SP-SEC-COMM-4-4: The OPC UA endpoint shall use mutual authentication via certificates. Note: OPC UA certificate validation is defined in ~~SPPRAMSS-18521~~ - *Missing cross-reference* Chapter 6.1.3 _ is implemented by: SP-SEC-Comp-5.4.2-2: The host-based firewall shall deny by default all inbound and outbound connections except for the designed network communications of the Secure Component. _ is implemented by: SP-SEC-Comp-5.4.2-1: The Secure Component shall provide the capability of a host-based firewall (e.g. packet filter using IP addresses, destination and source port, protocol and connection state (TCP) as filter parameter).

DRAFT

EU RED	Requirement	Implemented by
EU-RED-3-3e	(e): radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;	_ is implemented by: SP-SEC-Comp-5.3.3-1: If read access authorisation to persistent data is required, the Secure Component shall encrypt this data. Note: this applies at least for all confidential data at rest. It could be realized using file system encryption which encrypts all persistent data. _ is implemented by: SP-SEC-Comp-5.4.5-1: The Secure Component shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the Secure Component ('data minimisation').
EU-RED-3-3f	(f): radio equipment supports certain features ensuring protection from fraud;	
6 items found		

DRAFT

4 International standards

4.1 IEC 62443-2-1 (2024) compliance

The table contains all the 2-1 requirements with requirements number, short text and corresponding requirement or chapter in this doc.

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - ORG 1.1	Information security management system (ISMS)	_ is implemented by: SP-SEC-Pgrm-5-1: The railways shall implement an ISMS based on ISO 27001, chapter 4.4.
IEC 62443 2-1 - ORG 1.2	Background checks	_ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - ORG 1.3	Security roles and responsibilities	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-5-7: The railway shall define roles and responsibilities based on ISO 27002, chapter 5.2. _ is implemented by: 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 Secure Component based on ISO 27002 chapter 8.8.
IEC 62443 2-1 - ORG 1.4	Security awareness training	_ is implemented by: SP-SEC-Pgrm-5-10: The railway shall establish a security awareness and training program based on ISO 27002 chapter 6.3.
IEC 62443 2-1 - ORG 1.5	Security responsibilities training	_ is implemented by: SP-SEC-Pgrm-5-11: The railway shall establish security responsibilities training according to IEC 62443-2-1 Org 1.5.

DRAFT

IEC 62443 2-1 - ORG 1.6	Supply Chain Security	_ is implemented by: SP-SEC-Pgrm-5.1-3: The railway shall include security requirements in the supplier qualification process based on ISO 27002 chapter 5.19. _ is implemented by: 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). _ is implemented by: 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). _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: v: The railway shall define requirements for the availability of spare parts considering security related disturbances in the supply chain. _ is implemented by: SP-SEC-Pgrm-5.1-1: The railway shall implement supply chain security management based on ISO 27002 5.21. _ is implemented by: 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 Secure Component based on ISO 27002 chapter 8.8. _ is implemented by: v: The railway shall ensure that requirements related to the management of service providers are implemented by the supply chain. _ is implemented by: 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.

DRAFT

_ is implemented by: 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.

_ is implemented by: 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.

_ is implemented by: SP-SEC-Pgrm-13.2-2: The supplier shall implement supply chain security management.

Note: Recommended activities for supply chain management are document in IEC 62443-4-1 (SM-9, SM-10) and ISO 27002 5.21.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - ORG 2.1	Security risk mitigation	_ is implemented by: SP-SEC-Pgrm-5-12: The railway shall have policies and procedures for the management of risks based on ISO 27001 6.1.
IEC 62443 2-1 - ORG 2.2	Processes for discovery of security anomalies	_ is implemented by: 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 _ is implemented by: SP-SEC-Pgrm-5-15: The railway shall define procedures to check the system integrity. _ is implemented by: v: The railway shall check the system integrity after an interruption of the Secure Component's security monitoring. _ is implemented by: 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. _ is implemented by: 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)

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - ORG 2.3	Secure development and support	_ is implemented by: 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. _ is referred by: 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. _ is implemented by: SP-SEC-Pgrm-5-18: The railway shall implement secure development based on ISO 27002 8.25 for own developments and support. _ is implemented by: 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. _ is implemented by: 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. _ is referred by: SP-SEC-Pgrm-5-21: The railway shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10.
IEC 62443 2-1 - ORG 2.4	SP reviews	_ is implemented by: SP-SEC-Pgrm-13.1-2: The supplier shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10. _ is implemented by: SP-SEC-Pgrm-5-21: The railway shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - ORG 3.1	Physical access control	_ is implemented by: SP-SEC-Pgrm-5.2-7: For infrastructure, the railway shall choose the location of Secure Components considering industrial risks. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: 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). _ is implemented by: SP-SEC-Pgrm-5.1-17: The railway shall ensure that the tamper-evident seal of the component is checked prior to commissioning. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-5.2-6: For infrastructure, the railway shall choose the location of Secure Components considering risk of natural disasters.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - CM 1.1	Asset inventory baseline	_ is implemented by: 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..
IEC 62443 2-1 - CM 1.2	Infrastructure drawings/ documentation	_ is implemented by: 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 Secure 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 _ is implemented by: SP-SEC-Pgrm-6.1-2: The railway shall proof that all documentation is provided in electronic form. _ is implemented by: SP-SEC-Pgrm-6.1-4: The railway shall ensure that all documentation is kept up to date. _ is implemented by: 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) _ is implemented by: SP-SEC-Pgrm-6.1-3: The railway shall proof that all documentation referenced in chapter 14.4 was provided. _ is implemented by: SP-SEC-Pgrm-13.4-1: The supplier shall create technical documentation for each supplied Secure Component according to the requirements in SP-SEC-CompSpec Ch 6.3 - Product Documentation
IEC 62443 2-1 - CM 1.3	Configuration settings	_ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - CM 1.4	Change control	_ is implemented by: 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.
IEC 62443 2-1 - NET 1.1	Segmentation from non-IACS zones	_ is implemented by: 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.
IEC 62443 2-1 - NET 1.2	Documentation of zones and network zone interconnections	_ is implemented by: 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)
IEC 62443 2-1 - NET 1.3	Network segmentation from safety systems	_ is implemented by: 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.
IEC 62443 2-1 - NET 1.4	Network autonomy	_ is implemented by: IEC 62443 2-1 - ORG 2.2: Processes for discovery of security anomalies _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-7-4: The railway shall follow IEC 62443-2-1 Net 1.4, where applicable.
IEC 62443 2-1 - NET 1.5	Network disconnection from external networks	_ is implemented by: 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.
IEC 62443 2-1 - NET 1.6	Internal network access control	_ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - NET 1.7	Network accessible services	_ is implemented by: 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. _ is implemented by: 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].
IEC 62443 2-1 - NET 1.8	User messaging	_ is implemented by: SP-SEC-Pgrm-7-14: The railway shall hinder user-to-user messages by applying the principles of ISO 27002 chapter 8.20
IEC 62443 2-1 - NET 1.9	Network time distribution	_ is implemented by: SP-SEC-Pgrm-12.2-3: The railway shall distribute time securely as defined in the Shared Cybersecurity Specification SP-SEC-SERV CH 5
IEC 62443 2-1 - NET 2.1	Wireless protocols	_ is implemented by: 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.
IEC 62443 2-1 - NET 2.2	Wireless network segmentation	_ is implemented by: 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.
IEC 62443 2-1 - NET 2.3	Wireless properties and addresses	_ is implemented by: SP-SEC-Pgrm-7-17: If the railway uses wireless networks, the railway shall implement policies and procedures according to Net 2.3.
IEC 62443 2-1 - NET 3.1	Remote access applications	_ is implemented by: SP-SEC-Pgrm-7-10: Remote application access, besides 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - NET 3.2	Remote access connections	_ is implemented by: SP-SEC-Pgrm-7-10: Remote application access, besides 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.
IEC 62443 2-1 - NET 3.3	Remote access termination	_ is implemented by: SP-SEC-Pgrm-7-10: Remote application access, besides 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.
IEC 62443 2-1 - COMP 1.1	Component hardening	_ is implemented by: SP-SEC-Pgrm-8-5: The railway shall harden Secure Components prior to their use by applying the principles of ISO 27002 chapter 8.9.
IEC 62443 2-1 - COMP 1.2	Dedicated portable media	_ is implemented by: 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.
IEC 62443 2-1 - COMP 2.1	Malware free	_ is implemented by: SP-SEC-Pgrm-8-7: The railway shall require a confirmation by the supplier that the Secure Component is free of known malware before first use. _ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - COMP 2.2	Malware protection	_ is implemented by: SP-SEC-Pgrm-8-8: The railway shall realize malware protection for Secure Components through allow listing. _ is implemented by: SP-SEC-Pgrm-8-9: The railway shall define the allow-list to be used by the filter. Note: Malware protection via virus scanner is not applied as it is not feasible in the OT domain. _ is implemented by: SP-SEC-Pgrm-8-10: If malware protection shall be used for other components than Secure Components, the railway shall have policies and procedures related to malware protection availble based on ISO 27002 chapter 8.7.
IEC 62443 2-1 - COMP 2.3	Malware protection software validation and installation	_ is implemented by: SP-SEC-Pgrm-8-8: The railway shall realize malware protection for Secure Components through allow listing.
IEC 62443 2-1 - COMP 3.1	Security patch authenticity/integrity	_ is implemented by: 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.
IEC 62443 2-1 - COMP 3.2	Security patch validation and installation	_ is implemented by: 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. _ is implemented by: 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). _ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - COMP 3.3	Security patch status	_ is implemented by: 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. _ is implemented by: 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.
IEC 62443 2-1 - COMP 3.4	Security patching retention of security	_ is implemented by: IEC 62443-4-1 SUM-1: Verification of security updates addressing the intended security vulnerabilities, not introducing regressions. _ is implemented by: 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.
IEC 62443 2-1 - COMP 3.5	Security patch mitigation	_ is implemented by: 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 . _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-8.1-7: The railway shall calculate the CVSS v4.0 Base + Threat + Environment metric for all vulnerabilities.
IEC 62443 2-1 - DATA 1.1	Data classification	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9-2: The railway shall use the Traffic Light Protocol (TLP) 2.0 for classifying information.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - DATA 1.2	Data confidentiality	_ is implemented by: 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.
IEC 62443 2-1 - DATA 1.3	Safety system configuration mode	_ is implemented by: SP-SEC-Pgrm-8.1-21: The railway shall follow IEC 62443-2-1 DATA 1.3 for updating the Secure Component. _ is implemented by: SP-SEC-Pgrm-9-4: The railway shall have policies and procedures regarding the configuration of safety systems based on ISO 27002 8.32.
IEC 62443 2-1 - DATA 1.4	Data retention policy	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9-4: The railway shall have policies and procedures related to data retention based on ISO 27002 5.33. _ is implemented by: SP-SEC-Pgrm-9.2-3: The railway shall require and establish procedures to securely destroy equipment if purging data is not possible.
IEC 62443 2-1 - DATA 1.5	Cryptographic mechanisms	_ is implemented by: SP-SEC-Pgrm-9-7: The railway shall implement IEC 62443-2-1 Data 1.5.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - DATA 1.6	Key management	_ is implemented by: 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). _ is implemented by: 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). _ is implemented by: SP-SEC-Pgrm-9.1-4: The railway shall define the validity timespan of certificate revocation lists which was downloaded to the Secure Component. _ is implemented by: SP-SEC-Pgrm-9.1-2: The root CA operation shall operate the root CA offline. _ is implemented by: SP-SEC-Pgrm-9.2-4: The railway shall revoke certificates of the Secure Component during decommissioning process. _ is implemented by: 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.
IEC 62443 2-1 - DATA 1.7	Data integrity	_ is implemented by: SP-SEC-Pgrm-9.1-5: The railway shall define intervals for certificate validation according to operational need and security policy. _ is implemented by: SP-SEC-Pgrm-9-8: The railway shall implement IEC 62443-2-1 Data 1.7.
IEC 62443 2-1 - USER 1.1	User identity assignment	_ is implemented by: 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.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - USER 1.2	User identity removal	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9.2-8: If the decommissioning process fails, the railway shall require a procedure to securely manage the Secure Component and prevent any electronic interaction with the system when decommissioning process can not be accomplished or fails. _ is implemented by: SP-SEC-Pgrm-9.2-5: The railway shall remove all access rights of the Secure Component during decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.1-8: If the Secure Component is lost, the railway shall revoke any associated certificates. _ is implemented by: 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 . _ is implemented by: SP-SEC-Pgrm-9.1-7: If a Secure Component is decommissioned, the railway shall revoke any associated certificates.
IEC 62443 2-1 - USER 1.3	User identity persistence	_ is implemented by: SP-SEC-Pgrm-10-4: The railway shall define for which users automatic disabling of access rights shall not apply.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - USER 1.4	Access rights assignment	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-10-7: The railway shall assign permissions to roles in the IAM. _ is implemented by: SP-SEC-Pgrm-9.2-6: The railway shall change the status of the Secure Component in the asset management system to "to be decommissioned" before decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.2-7: The railway shall change the status of the Secure Component in the asset management system to "decommissioned" after successful decommissioning process. _ is implemented by: SP-SEC-Pgrm-10-6: The railway shall assign users to roles in the IAM. _ is implemented by: SP-SEC-Pgrm-10-8: The railway shall define a re-certification process for users. _ is implemented by: 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.
IEC 62443 2-1 - USER 1.5	Least privilege	_ is implemented by: SP-SEC-Pgrm-9.2-10: The railway shall follow the least privilege principle for assigning users and roles. _ is implemented by: SP-SEC-Pgrm-10-13: The railway shall grant physical access based on the least-privilege-principle.
IEC 62443 2-1 - USER 1.6	Software service authentication	_ is implemented by: 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.
IEC 62443 2-1 - USER 1.7	Software interactive login rights	_ is implemented by: SP-SEC-Pgrm-10-15: The railway shall deny interactive login capabilities for technical identities.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - USER 1.8	Human user authentication	_ is implemented by: SP-SEC-Pgrm-10-16: The railway shall ensure that every user (human users, software processes or devices) is a unique identity.
IEC 62443 2-1 - USER 1.9	Multifactor authentication (MFA)	_ is implemented by: 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.
IEC 62443 2-1 - USER 1.10	Mutual authentication	_ is implemented by: SP-SEC-Pgrm-10-18: The railway shall apply procedures and policies to use the mutual authentication mechanisms defined in the Secure Component Specification.
IEC 62443 2-1 - USER 1.11	Password protection	_ is implemented by: : 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). _ is implemented by: SP-SEC-Pgrm-10-21: The railway shall establish password policies and procedures for human users based on ISO 27002 chapter 5.7.
IEC 62443 2-1 - USER 1.2	Shared and disclosed/ compromised passwords	_ is implemented by: SP-SEC-Pgrm-10-26: The railway shall ensure unique user identification by denying shared credentials. _ is implemented by: 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.
IEC 62443 2-1 - USER 1.13	User login display information	_ is implemented by: SP-SEC-Comp-7.2-8: If the Secure Component implements a human-machine interface with interactive log-in, the log-in screen shall be configurable to provide information about user log-in histories and recently failed log-in attempts according to IEC 62443-2-1 User 1.13.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - USER 1.14	User login failure displays	_ is implemented by: SP-SEC-Comp-7.2-9: If the Secure Component implements a human-machine interface with interactive log-in, the log-in screen shall display log-in failure information only after successful login. Note: this prevents to display useful information to attackers (see also IEC 62443-2-1 USER-1.14)
IEC 62443 2-1 - USER 1.15	Consecutive login failures	_ is implemented by: 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.
IEC 62443 2-1 - USER 1.16	Session integrity	_ is implemented by: 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".
IEC 62443 2-1 - USER 1.17	Concurrent sessions	_ is implemented by: 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.
IEC 62443 2-1 - USER 1.18	Screen lock	_ is implemented by: SP-SEC-Comp-7.2-4: If the Secure Component provides a human-machine interface, the Secure Component shall lock or terminate sessions after a time period of inactivity depending on configuration. _ is implemented by: 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. _ is implemented by: 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.]
IEC 62443 2-1 - USER 1.19	Component authentication	_ is implemented by: 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.
IEC 62443 2-1 - USER 2.1	Authorization	_ is implemented by: SP-SEC-Pgrm-10-34: The railway shall define policies and procedures regarding access rights based on ISO 27002 8.3

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - USER 2.2	Separation of duties	_ is implemented by: SP-SEC-Pgrm-10-27: The railway shall define policies and procedures related to separation of duties based on ISO 27002 5.3 _ is implemented by: SP-SEC-Pgrm-10-19: The railway shall define roles following the segregation of duties principle.
IEC 62443 2-1 - USER 2.3	Multiple approvals	_ is implemented by: 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 _ is implemented by: 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
IEC 62443 2-1 - USER 2.4	Manual elevation of privileges	_ is implemented by: 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.
IEC 62443 2-1 - EVENT 1.1	Event detection	_ is implemented by: 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.
IEC 62443 2-1 - EVENT 1.2	Event reporting	_ is implemented by: SP-SEC-Pgrm-11-12: The railway shall apply the defined interfaces by the Secure Communication and Shared Cybersecurity Specification to report events.
IEC 62443 2-1 - EVENT 1.3	Event reporting interfaces	_ is implemented by: SP-SEC-Pgrm-11-12: The railway shall apply the defined interfaces by the Secure Communication and Shared Cybersecurity Specification to report events.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - EVENT 1.4	Logging	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-11-1: The railway shall define a logging strategy, integrating legacy and new systems.
IEC 62443 2-1 - EVENT 1.5	Log entries	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-11-1: The railway shall define logging requirements based on ISO 27002 chapter 8.15.
IEC 62443 2-1 - EVENT 1.6	Log access	_ is implemented by: SP-SEC-Pgrm-11-12: The railway shall apply the defined interfaces by the Secure Communication and Shared Cybersecurity Specification to report events. _ is implemented by: 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.
IEC 62443 2-1 - EVENT 1.7	Event analysis	_ is implemented by: 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.
IEC 62443 2-1 - EVENT 1.8	Incident handling and response	_ is implemented by: SP-SEC-Pgrm-11-13: The railway shall define an incident handling and response process based on ISO 27002 chapter 5.26.

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - EVENT 1.9	Vulnerability handling	_ is implemented by: SP-SEC-Pgrm-8.1-2: The railway shall require the suppliers to follow a coordinated vulnerability disclosure procedure according to ISO 29147. _ is implemented by: SP-SEC-Pgrm-8.1-5: The railway shall define procedures for the vulnerability management process of the Secure Component based on ISO 27002 chapter 8.8. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-11-1: The railway shall implement a vulnerability management process.
IEC 62443 2-1 - AVAIL 1.1	Continuity management	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-12.1-1: The railway shall define and implement a disaster recovery plan. _ is implemented by: SP-SEC-Pgrm-12.1-2: The railway shall test the disaster recovery plan in a self defined repetition rate.
IEC 62443 2-1 - AVAIL 1.2	Resource availability management	_ is implemented by: SP-SEC-Pgrm-12.1-4: The railway shall have a resource availability and redundancy management based on ISO 27002 8.14
IEC 62443 2-1 - AVAIL 1.3	Failure-state	_ is implemented by: 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
IEC 62443 2-1 - AVAIL 2.1	Backup	_ is implemented by: SP-SEC-Pgrm-12.3-1: The railway shall have policies and procedures for backup and restore based on ISO 27002 8.13

DRAFT

IEC 62443-2-1	Requirement	Implemented by
IEC 62443 2-1 - AVAIL 2.2	Backup non-interference	_ is implemented by: 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.
IEC 62443 2-1 - AVAIL 2.3	Backup verification	_ is implemented by: SP-SEC-Pgrm-12.3-1: The railway shall have policies and procedures for backup and restore based on ISO 27002 8.13
IEC 62443 2-1 - AVAIL 2.4	Backup media	_ is implemented by: SP-SEC-Pgrm-12.3-1: The railway shall have policies and procedures for backup and restore based on ISO 27002 8.13
IEC 62443 2-1 - AVAIL 2.5	Backup restoration	_ is implemented by: SP-SEC-Pgrm-12.3-1: The railway shall have policies and procedures for backup and restore based on ISO 27002 8.13
88 items found		

4.2 IEC 62443-4-2 compliance

The table contains all the 4-2 requirements (SL1 to SL4) with requirements number, short text and corresponding requirement or chapter in this doc.

4.2.1 Rationale for not considered requirements from IEC 62443-4-2

NOT IMPLEMENTED: **CR 1.7 RE 2**:
Password life-time restrictions for all users (human, software processes and devices).

Technical users do not use passwords, but certificates instead. Human users have separate requirements for password life-time restrictions. Requirement not needed.

NOT IMPLEMENTED: **CR 1.12**.
System use notification is required by US law for legal prosecution of violators and proving intentional breach.

This is not required in the EU legislation (not in EU-NIS2, EU-CSA, EU CRA, EU RED).

NOT IMPLEMENTED: **EDR/NDR/HDR 2.13 RE1**:
Active monitoring of physical factory diagnostic and test interfaces if they are disabled, creation of a log for access attempts.

DRAFT

Monitoring these interfaces (e.g. JTAG) does not provide additional security (since there are numerous other attacks when the attacker has physical access to the component, e.g. installing own probes).

NOT IMPLEMENTED: **HDR 3.2 RE 1**:
Reporting the version of software and files for code protection only is applicable for anti-virus solution, which is not advised to use in automation products for protection against malware.

This specification uses a runtime-integrity checks for software processes to protect against the execution unauthorised software. See SP-SEC-CompSpec Ch 5.3.1 Process runtime-integrity check

NOT IMPLEMENTED: **CR 3.9 RE 1**:
Using hardware-enforced write-once media to store audit records.

This SL4 requirement requires specialized hardware and does not provide a beneficial cost to security enhancement ratio. A more cost-effective solution to protect audit information from attackers is to install an isolated log server and connect it via a network tap (shadow logging) to the supervised network communication. This prevents an attacker to gain access to the shadow log server.

DRAFT

4.2.2 Tracing to IEC 62443-4-2

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CCSC 1	Support for essential functions	_ is implemented by: SP-SEC-Comp-5.4.4-2: After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally. Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds. This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1 _ is implemented by: SP-SEC-Comp-7.2-7: If the Secure Component implements a human-machine interface which is needed to control an essential service, the Secure Component shall support a supervisor manual override for a configurable time or sequence of events. _ is implemented by: SP-SEC-Comp-5.4.4-1: The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion. Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits.
IEC 62443-4-2 CCSC 2	Compensating countermeasures	_ is implemented by: SP-SEC-Comp-2.2-3: If a requirement of this specification cannot be implemented (yet), the component documentation shall provide a justification for each non-implemented requirement, with respect to organisational needs, operational constraints and regulatory requirements (e.g. interface is not needed for operation, alternative mitigation, justified by an impact / risk analysis). _ is implemented by: SP-SEC-Comp-2.2-4: If a requirement of this specification cannot be implemented (yet), the component documentation shall include a description how to handle this case which has to be agreed with the asset owner (e.g. definition of a security related application condition).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CCSC 3	Least privilege	_ is implemented by: SP-SEC-Comp-7.2-2: If the Secure Component provides a human-machine interface, the Secure Component shall enforce the permissions received from the UAS service via SSI-UAS for the corresponding communication session. _ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-CommExt-1.4-4: Each software process realizing an additional communication interface shall enforce access based on retrieved permissions. Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. _ is implemented by: SP-SEC-Comp-5.5.3-7: The Secure Component shall validate and enforce the extended key usage according to the definition in SP-SEC-ServSpec Ch 14.1 Certificate Profiles. _ is implemented by: SP-SEC-Pgrm-9.2-10: The railway shall follow the least privilege principle for assigning users and roles. _ is implemented by: SP-SEC-Comm-6-2: The communication endpoint shall validate the certificate algorithms, key lengths, profile, Key Usage and Extended Key Usage according to the definition in Shared Cybersecurity Services Specification Chapter 14.1 Certificate Profiles.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CCSC 4	Software development process	_ is implemented by: SP-SEC-Comp-5.1-1: The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum). Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence). Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security)
IEC 62443-4-2 CR 1.01	Human user identification and authentication	_ is implemented by: SP-SEC-Comp-7.2-1: If the Secure Component provides a human-machine interface, the Secure Component shall support human user authentication and authorization via SSI-UAS. _ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.01 RE 1	Unique identification and authentication	_ is implemented by: SP-SEC-Comp-7.2-1: If the Secure Component provides a human-machine interface, the Secure Component shall support human user authentication and authorization via SSI-UAS. _ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable. _ is implemented by: SP-SEC-Serv-10-9: The SCS-UAS shall support authentication with X.509 client certificates complying to the Operator User Certificate (OUC) profile see ~~SPPRAMSS-7651~~ - *Missing cross-reference*.
IEC 62443-4-2 CR 1.01 RE 2	Multifactor authentication for all interfaces	_ is implemented by: SP-SEC-Serv-10-3: The SCS-UAS shall support multi-factor authentication of human users. _ is implemented by: SP-SEC-Serv-10-10: The SCS-UAS shall support authentication with username/password with at least one additional factor (e.g. authenticator apps using TOTP (time-based one-time-password)). _ is implemented by: SP-SEC-Serv-10-9: The SCS-UAS shall support authentication with X.509 client certificates complying to the Operator User Certificate (OUC) profile see ~~SPPRAMSS-7651~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-Serv-10-11: The SCS-UAS should support passwordless authentication with at least one additional factor (e.g. passkeys with biometric factor).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.02	Software process and device identification and authentication	_ is implemented by: SP-SEC-Comp-5.5.2-10: The Secure Component shall support certificates defined in SP-SEC-ServSpec Ch 14.1 - Certificate Profiles. _ is implemented by: SP-SEC-CommExt-1.4-1: Each software process realising an additional communication interface shall be capable of identifying itself and authenticating to any other communication partner using a unique X.509 v3 certificate as defined in ☐ ~~SPPRAMSS-2031~~ - *Missing cross-reference* or an equally secure method. Note1: recommendation is to use a unique X.509 certificate Note2: there should be a way to identify a software process (web server, safety communication, diagnostics server,...), not per software process instance of the same software process. _ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable. _ is implemented by: SP-SEC-Comp-5.5.4-9: The Secure Component shall request the Operator Device Certificate (ODC) via the SSI-PKI interface using the Manufacturer Device Certificate (MDC) for message protection. _ is implemented by: SP-SEC-Comp-5.5.4-4: The Secure Component shall be equipped with a Manufacturer Device Certificate (MDC) which includes the unique serial number of the Secure Component as described in SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile. _ is implemented by: SP-SEC-Comp-5.5.2-11: If more than one network interface is used for safety communication, the Secure Component shall use a dedicated OSCC for each network interface. Note: this ensures that if the communication certificate of one network interface is renewed, the connection over the other network interface maintains its independency.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.02 RE 1	Unique identification and authentication	_ is implemented by: SP-SEC-COMM-3.2-1: The TLS endpoint shall perform authentication using certificates in accordance with X.509 (~~SPPRAMSS-2031~~ - *Missing cross-reference*). _ is implemented by: SP-SEC-COMM-4-4: The OPC UA endpoint shall use mutual authentication via certificates. Note: OPC UA certificate validation is defined in ~~SPPRAMSS-18521~~ - *Missing cross-reference* Chapter 6.1.3 _ is implemented by: SP-SEC-CommExt-1.4-1: Each software process realising an additional communication interface shall be capable of identifying itself and authenticating to any other communication partner using a unique X.509 v3 certificate as defined in ~~SPPRAMSS-2031~~ - *Missing cross-reference* or an equally secure method. Note1: recommendation is to use a unique X.509 certificate Note2: there should be a way to identify a software process (web server, safety communication, diagnostics server,...), not per software process instance of the same software process. _ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable. _ is implemented by: SP-SEC-Comp-5.5.4-9: The Secure Component shall request the Operator Device Certificate (ODC) via the SSI-PKI interface using the Manufacturer Device Certificate (MDC) for message protection. _ is implemented by: SP-SEC-Comp-5.5.4-10: The Secure Component shall request all other operator certificates (ONCC, OSCC, OUC, OCSC, see SP-SEC-ServSpec Ch 5.1.3 - Use Case: Updating Operator Certificates) via the SSI-PKI interface using the Operator Device Certificate (ODC) for message protection. _ is implemented by: SP-SEC-Comp-5.5.4-4: The Secure Component shall be equipped with a Manufacturer Device Certificate (MDC) which includes the unique serial number of the Secure Component as described in SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.03	Account management	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-Comm-4-13: The OPC UA endpoint shall enforce permissions retrieved via the SSI-IAM interface. _ is implemented by: SP-SEC-Serv-7.2-1: The SSI-IAM shall provide access to its user inventory via SCIM under the endpoint `/v2/Users`.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.04	Identifier management	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-Comp-5.5.4-10: The Secure Component shall request all other operator certificates (ONCC, OSCC, OUC, OCSC, see SP-SEC-ServSpec Ch 5.1.3 - Use Case: Updating Operator Certificates) via the SSI-PKI interface using the Operator Device Certificate (ODC) for message protection. _ is implemented by: SP-SEC-Serv-7.1-1: The SSI-IAM server shall provide access to its asset inventory via SCIM 2.0 under the endpoint `/v2/Assets`.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.05	Authenticator management	_ is implemented by: SP-SEC-Comp-5.5.2-5: The Secure Component shall automatically request the renewal of its certificates a configurable number of days in advance to the certificate's expiration date. Note: after rekeying a certificate, it is recommended to not revoke the old certificate to keep CRLs manageable. _ is implemented by: SP-SEC-Comp-5.2.3-1: The Secure Component shall protect the integrity and confidentiality of critical and long-life private and symmetric keys via a commonly accepted cryptographic mechanism originating from hardware. _ is implemented by: SP-SEC-Comp-5.5.4-9: The Secure Component shall request the Operator Device Certificate (ODC) via the SSI-PKI interface using the Manufacturer Device Certificate (MDC) for message protection. _ is implemented by: SP-SEC-Comp-5.5.4-10: The Secure Component shall request all other operator certificates (ONCC, OSCC, OUC, OCSC, see SP-SEC-ServSpec Ch 5.1.3 - Use Case: Updating Operator Certificates) via the SSI-PKI interface using the Operator Device Certificate (ODC) for message protection. _ is implemented by: SP-SEC-Comp-5.5.5-1: The Secure Component shall have the capability to install trusted certificates in the trust store via the mechanism described in Chapter SP-SEC-CompSpec Ch 5.6.1 - Software Update. _ is implemented by: SP-SEC-Comp-5.5.4-4: The Secure Component shall be equipped with a Manufacturer Device Certificate (MDC) which includes the unique serial number of the Secure Component as described in SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile.
IEC 62443-4-2 CR 1.05 RE 1	Hardware security for authenticators	_ is implemented by: SP-SEC-Comp-5.2.3-1: The Secure Component shall protect the integrity and confidentiality of critical and long-life private and symmetric keys via a commonly accepted cryptographic mechanism originating from hardware. _ is implemented by: SP-SEC-Comp-5.2.3-2: The Secure Component shall protect the integrity of roots of trust (root certificates) via a commonly accepted cryptographic mechanism originating from hardware. Note: examples of commonly accepted cryptographic mechanism originating from hardware are trusted execution environment (TEE), trusted platform module (TPM 2.0 or higher), hardware security module (HSM).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.07	Strength of password-based authentication	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-Comp-7.3-2: If the Secure Component supports local password-based authentication and local user management, then Secure Component shall enforce configurable password strength (minimum length, variety of character types). _ is implemented by: SP-SEC-Comp-6.2-4: If the Secure Component supports local password-based authentication, the Secure Component shall provide following configuration items: • password rules (minimum length, variety of character types) • number of generations before reusing a password • minimum and maximum password lifetime • number of consecutive invalid access attempts • time period to deny access when the limit of consecutive invalid login attempts has been reached • number of days before password expiration to prompt the human user to change their password Note 1: The Secure Component implementing the SSI-UAS service should support password-based authentication and the password configuration items. Note 2: Secure Components using user authentication via the SSI-UAS interface do not need to support password-based authentication or password configuration items. Note 3: Common security practices recommend to only change passwords when there is an indication of compromise. Therefore, the maximum password lifetime should be set to infinite (e.g. a long time in the future).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.07 RE 1	Password generation and lifetime restrictions for human users	_ is implemented by: SP-SEC-Comp-7.3-4: If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall provide the capability to enforce password minimum and maximum lifetime restrictions for all human users. _ is implemented by: SP-SEC-Comp-7.3-3: If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall provide the capability to protect against any given human user account from reusing a password for a configurable number of generations.
IEC 62443-4-2 CR 1.07 RE 2	Password lifetime restrictions for all users (human, software process, or device...	_ is implemented by: : NOT IMPLEMENTED: **CR 1.7 RE 2**: Password life-time restrictions for all users (human, software processes and devices). Technical users do not use passwords, but certificates instead. Human users have separate requirements for password life-time restrictions. Requirement not needed.
IEC 62443-4-2 CR 1.08	Public key infrastructure certificates	_ is implemented by: SP-SEC-Comp-5.5.2-4: The Secure Component shall implement the interface SP-SEC-ServSpec Ch 5 - PKI: Public Key Infrastructure to renew a certificate. _ is implemented by: SP-SEC-Comp-5.5.2-1: The Secure Component shall implement the interface SP-SEC-ServSpec Ch 6 - Public Key Infrastructure to request certificates.

DRAFT

IEC 62443-4-2 CR 1.09	Strength of public key-based authentication	_ is implemented by: SP-SEC-COMM-3.1-1: The TLS endpoint shall use TLS version 1.3 as defined in ~~SPPRAMSS-1698~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-COMM-3.1-3: The TLS endpoint shall enforce mutual authentication. _ is implemented by: SP-SEC-COMM-4-4: The OPC UA endpoint shall use mutual authentication via certificates. Note: OPC UA certificate validation is defined in ~~SPPRAMSS-18521~~ - *Missing cross-reference* Chapter 6.1.3 _ is implemented by: SP-SEC-COMM-4-2: The OPC UA endpoint shall use Secure Conversation (UASC) (~~SPPRAMSS-2957~~ - *Missing cross-reference* , Chapter 6.7) _ is implemented by: SP-SEC-COMM-4-3: The OPC UA endpoint shall use SignAndEncrypt as security mode. _ is implemented by: SP-SEC-Comm-6-1: The communication endpoint using certificate-based authentication shall validate certificates according to X.509 as defined in ~~SPPRAMSS-2031~~ - *Missing cross-reference* Chapter 6. Note: the RFC 5280 defines the validation of the certificate's trust chain up to a trusted certificate authority and how to check the certificate validity periods in the certificate path. _ is implemented by: SP-SEC-Comm-6-4: The communication endpoint shall map the authenticated identity of a certificate to a device, software process, technical user or human user, depending on the communication use case. Note: The mapped identity is to be used for authorization decisions. _ is implemented by: SP-SEC-Comm-6-2: The communication endpoint shall validate the certificate algorithms, key lengths, profile, Key Usage and Extended Key Usage according to the definition in Shared Cybersecurity Services Specification Chapter 14.1 Certificate Profiles. _ is implemented by: SP-SEC-Comm-6-6: The communication endpoint shall check the revocation status of each certificate in the certificate path using Certificate Revocation Lists according to [RFC 5280] Chapter 6.3. Note: Self-signed certificates (e.g. trust anchors) do not have a revocation status which can be validated. RFC 5280 defines checks for the following conditions: ◦ the CRL signature is valid; ◦ the CRL issuer is the expected certificate authority; ◦ the CRL can be linked to the certificate issuer; ◦ the current time is within the CRL validity period; ◦ the current time is earlier than or equal to the CRL nextUpdate value; ◦ the CRL applies to the certificate being validate

DRAFT

_ is implemented by: SP-SEC-Comm-6-3: The communication endpoint shall establish that the communication partner controls the private key corresponding to the public key contained in the authenticated certificate.
Note: this requirement is fulfilled by TLS and OPC UA SC specifications and implementations.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.09 RE 1	Hardware security for public key-based authentication	_ is implemented by: SP-SEC-Comp-5.2.3-1: The Secure Component shall protect the integrity and confidentiality of critical and long-life private and symmetric keys via a commonly accepted cryptographic mechanism originating from hardware.
IEC 62443-4-2 CR 1.10	Authenticator feedback	_ is implemented by: SP-SEC-Comp-7.3-9: If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall obscure feedback of authentication information. Note: In case of invalid username/password combination, the feedback is invalid username/password combination, not give hints that could help an attacker as "invalid user" or "invalid password", "password length insufficient".

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.11	Unsuccessful login attempts	_ is implemented by: SP-SEC-Comp-7.3-6: If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall limit the number of consecutive invalid access attempts by any user (human or technical user). _ is implemented by: SP-SEC-Comp-6.2-4: If the Secure Component supports local password-based authentication, the Secure Component shall provide following configuration items: • password rules (minimum length, variety of character types) • number of generations before reusing a password • minimum and maximum password lifetime • number of consecutive invalid access attempts • time period to deny access when the limit of consecutive invalid login attempts has been reached • number of days before password expiration to prompt the human user to change their password Note 1: The Secure Component implementing the SSI-UAS service should support password-based authentication and the password configuration items. Note 2: Secure Components using user authentication via the SSI-UAS interface do not need to support password-based authentication or password configuration items. Note 3: Common security practices recommend to only change passwords when there is an indication of compromise. Therefore, the maximum password lifetime should be set to infinite (e.g. a long time in the future). _ is implemented by: SP-SEC-Comp-7.3-8: If the Secure Component supports local password-based authentication and local user management and user accounts can be locked (e.g. due consecutive invalid access attempts), then the Secure Component shall be capable to unlock a locked account by an administrator _ is implemented by: SP-SEC-Comp-7.3-7: If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall deny access for a specific period of time when the limit of consecutive invalid attempts is reached.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 1.12	System use notification	_ is implemented by: : NOT IMPLEMENTED: **CR 1.12**. System use notification is required by US law for legal prosecution of violators and proving intentional breach. This is not required in the EU legislation (not in EU-NIS2, EU-CSA, EU CRA, EU RED).
IEC 62443-4-2 CR 1.14	Strength of symmetric key-based authentication	_ is implemented by: SP-SEC-Comp-5.2.3-1: The Secure Component shall protect the integrity and confidentiality of critical and long-life private and symmetric keys via a commonly accepted cryptographic mechanism originating from hardware. _ is implemented by: SP-SEC-Comp-7.4-1: If symmetric key-based authentication is used, the Secure Component shall establish the mutual trust using the symmetric key. _ is implemented by: SP-SEC-Comp-7.4-2: If symmetric key-based authentication is used due to interoperability requirements by TSI, the Secure Component shall protect the symmetric key-based authentication by another security layer conformant to chapter 4 of the Secure Communication Specification (SP-SEC-Comm Ch 3 - End-to-End Security Layer (TLS) .) Note 1: the use of symmetric key-based authentication requires the distribution of the symmetric keys ensuring confidentiality. This can be done using PKI / asymmetric cryptography or a out-of-band transmission ensuring confidentiality. Note 2: Symmetric key authentication does not conform to internationally recognized and proved security practices. The only reason to implement it, may be the TSI. In this case, the appropriate security will be provided by adding a second security layer which uses industry-wide accepted security mechanism. This is, for example, done with the ETCS communication with Subset-146 for symmetric cipher of Subset-137-2)
IEC 62443-4-2 CR 1.14 RE 1	Hardware security for symmetric key-based authentication	_ is implemented by: SP-SEC-Comp-5.2.3-1: The Secure Component shall protect the integrity and confidentiality of critical and long-life private and symmetric keys via a commonly accepted cryptographic mechanism originating from hardware.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.01	Authorization enforcement	_ is implemented by: SP-SEC-CommExt-1.4-4: Each software process realizing an additional communication interface shall enforce access based on retrieved permissions. Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. _ is implemented by: SP-SEC-Comm-4-13: The OPC UA endpoint shall enforce permissions retrieved via the SSI-IAM interface.
IEC 62443-4-2 CR 2.01 RE 1	Authorization enforcement for all users (human, software process, and devices)	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization. Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication. Note2: in case of non-availability of the IAM, local accounts can be used _ is implemented by: SP-SEC-CommExt-1.4-4: Each software process realizing an additional communication interface shall enforce access based on retrieved permissions. Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. _ is implemented by: SP-SEC-Comm-4-13: The OPC UA endpoint shall enforce permissions retrieved via the SSI-IAM interface.

DRAFT

IEC 62443-4-2 CR 2.01 RE 2	Permission mapping to roles	_ is implemented by: SP-SEC-CommExt-1.4-3: Each software process realizing an additional communication interface shall use the interface **[SSI-IAM]** to retrieve the permissions for a specified user (human or technical user) for non-token-based authentication or use interface **[SSI-UAS]** to retrieve permission for token-based authorization.
		
		Note1: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTPS, SSH,...), but not applicable for safety-relevant communication / M2M communication.
		Note2: in case of non-availability of the IAM, local accounts can be used
		_ is implemented by: SP-SEC-Comm-4-13: The OPC UA endpoint shall enforce permissions retrieved via the SSI-IAM interface.
		_ is implemented by: SP-SEC-Serv-7.2-5: If the SSI-IAM can provide the requested user permissions, the SSI-IAM server shall return a SCIM response with the schema `urn:ietf:params:scim:api:messages:2.0:ListResponse`, containing `Resources` of the schema `urn:ietf:params:scim:core:2.0:User`, which includes the users email addresses as values in the "emails" resource and the users permissions as values in the "entitlements" resource.
		Note 1: such a response has the following form:
		`HTTP/1.1 200 OK`
		`Content-Type: application/scim+json`
		`{`
		`"schemas":["urn:ietf:params:scim:api:messages:2.0:ListResponse"],`
		`"totalResults":1,`
		`"Resources": [`
		`{`
		`"id":"2819c223-7f76-453a-919d-413861904646",`
		`"schemas":["urn:ietf:params:scim:core:2.0:User"],`
		`"externalId":"jbloggs",`
		`"meta":{`
		`"resourceType":"User",`
		`"created":"2011-08-01T18:29:49.793Z",`
		`"lastModified":"2011-08-01T18:29:49.793Z",`
		`"location":`
		`"https://example.com/v2/Users/2819c223-7f76-453a-919d-13861904646",`
		`"version":"W\/\"f250dd84f0671c3\""`
		`},`

DRAFT

```
            "emails":[
                {"value":"joe.bloggs@example.com"}
            ],
            "entitlements": [
               {"value": "eu.rail.sdi.diagnostic-read"},
               {"value": "eu.rail.ssi.security-read"}
            ]
        ],
  }
  ]
}
```

Note 2: additional attributes are allowed

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.01 RE 3	Supervisor override	_ is implemented by: SP-SEC-Comp-7.2-7: If the Secure Component implements a human-machine interface which is needed to control an essential service, the Secure Component shall support a supervisor manual override for a configurable time or sequence of events.
IEC 62443-4-2 CR 2.01 RE 4	Dual approval	_ is implemented by: SP-SEC-Comp-7.2-3: If a Secure Components implementing a Shared Cybersecurity Service with a human-machine interface (e.g. IAM, software update system) allows high-risk operations, the Secure Components implementing a Shared Cybersecurity Service shall be capable to enforce the dual control principle. Note. Examples for high-risk operations are: assign admin role, update security configuration or software.
IEC 62443-4-2 CR 2.02	Wireless use control	_ is implemented by: SP-SEC-Comp-7.1.4-1: If a Network Component supports wireless access management (e.g. WLAN access point), the Network Component shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication with a control system. Note: this can be achieved using IEEE 802.1x EAP TLS.
IEC 62443-4-2 CR 2.05	Session lock	_ is implemented by: SP-SEC-Comp-7.2-4: If the Secure Component provides a human-machine interface, the Secure Component shall lock or terminate sessions after a time period of inactivity depending on configuration. _ is implemented by: SP-SEC-Comp-7.2-6: If the Secure Component provides a human-machine interface, the Secure Component shall unlock the locked human-user sessions only after re-authentication of the human user. Note: See also SP-SEC-Comp-7.2-7 for supervisor override in case of HMI controlling essential services.
IEC 62443-4-2 CR 2.06	Remote session termination	_ is implemented by: SP-SEC-Comp-7.2-4: If the Secure Component provides a human-machine interface, the Secure Component shall lock or terminate sessions after a time period of inactivity depending on configuration. _ is implemented by: SP-SEC-Comp-7.2-5: If the Secure Component provides a human-machine interface, the Secure Component shall enable the human user to lock or terminate sessions manually.
IEC 62443-4-2 CR 2.07	Concurrent session control	_ is implemented by: SP-SEC-Comp-5.4.4-3: The Secure Component shall provide the capability to only allow a configurable maximum number of concurrent sessions per interface for any given user (human, or technical user).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.08	Auditable events	_ is implemented by: SP-SEC-Comp-5.7.1-3: The Secure Component shall send log messages complying to the log message format defined in SP-SEC-ServSpec Ch 9.1 - Log Message Format Note: This ensures that the log messages contain the following data: a) timestamp (synchronized); b) source (originating device, software process or human user account); c) category; d) type; e) event ID; and f) event result _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).
IEC 62443-4-2 CR 2.09	Audit storage capacity	_ is implemented by: SP-SEC-Comp-5.7.1-6: If the storage capacity is exceeded, the Secure Component shall overwrite the oldest log entry first. _ is implemented by: SP-SEC-Comp-5.7.1-4: The Secure Component shall be able to store untransferred log data for eight hours or longer, up to the maximum available or reserved capacity. Note: These untransferred logs are accessible using the maintenance method described in SP-SEC-Serv Ch 12.3 - Log Maintenance . The untransferred logs are assumed to be accessible until a restart / reboot.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.09 RE 1	Warn when audit record storage capacity threshold reached	_ is implemented by: SP-SEC-Comp-5.7.1-7: If the storage capacity has reached a defined threshold, the Secure Component shall indicate this on its diagnostic interface and send it via SSI-LOG.
IEC 62443-4-2 CR 2.10	Response to audit processing failures	_ is implemented by: SP-SEC-Comp-5.7.1-6: If the storage capacity is exceeded, the Secure Component shall overwrite the oldest log entry first. _ is implemented by: SP-SEC-Comp-5.7.1-7: If the storage capacity has reached a defined threshold, the Secure Component shall indicate this on its diagnostic interface and send it via SSI-LOG.
IEC 62443-4-2 CR 2.11	Timestamps	_ is implemented by: SP-SEC-Comp-5.7.1-1: The Secure Component shall send the logging events via SSI-LOG SP-SEC-ServSpec Ch 9 - LOG: Security Logging . Note: this ensures encryption of the log messages and ensures that no information is provided that can be exploited by adversaries to attack the system. _ is implemented by: SP-SEC-Serv-9.1.2-11: The log originator shall set the timestamp of the syslog header to the current time as defined in ~~SPPRAMSS-13763~~ - *Missing cross-reference* using UTC date/time format including milliseconds using TIME-SECFRAC. Note: An Example for for such a timestamp is `2038-01-19T:03:14:08.000Z`
IEC 62443-4-2 CR 2.11 RE 1	Time synchronization	_ is implemented by: SP-SEC-Comp-5.3.7-1: The Secure Component shall synchronize the component time using **SSI-STS** secure time synchronization interface (refer to SP-SEC-ServSpec Ch 4 - STS: Secure Time Synchronisation).
IEC 62443-4-2 CR 2.11 RE 2	Protection of time source integrity	_ is implemented by: SP-SEC-Comp-5.3.7-1: The Secure Component shall synchronize the component time using **SSI-STS** secure time synchronization interface (refer to SP-SEC-ServSpec Ch 4 - STS: Secure Time Synchronisation). _ is implemented by: SP-SEC-Serv-5.3-1: The SSI-STS client shall use NTS as specified in ~~SPPRAMSS-3704~~ - *Missing cross-reference* . Note: This means, that at least TLS version 1.3 is used.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.12	Non-repudiation	_ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 2.12 RE 1	Non-repudiation for all users	_ is implemented by: SP-SEC-Comp-5.7.1-3: The Secure Component shall send log messages complying to the log message format defined in SP-SEC-ServSpec Ch 9.1 - Log Message Format Note: This ensures that the log messages contain the following data: a) timestamp (synchronized); b) source (originating device, software process or human user account); c) category; d) type; e) event ID; and f) event result _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.01	Communication integrity	_ is implemented by: SP-SEC-COMM-3.1-1: The TLS endpoint shall use TLS version 1.3 as defined in ~~SPPRAMSS-1698~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-COMM-4-2: The OPC UA endpoint shall use Secure Conversation (UASC) (~~SPPRAMSS-2957~~ - *Missing cross-reference* , Chapter 6.7) _ is implemented by: SP-SEC-Comp-5.5.1-2: The Secure Component shall implement the mandatory interfaces defined in [SP-SEC-ServSpec] Table 1. It may need to implement additional optional interfaces defined in [SP-SEC-ServSpec]for its specified function or standard communication protocols defined in [SP-SEC-CommSpec]. Note 1: This ensures the identification, authentication, integrity, and confidentiality requirements, as well as the first step of authorisation for network based communication for interfaces defined in Shared Cybersecurity Services Specification. For all other communication interfaces, the requirements are listed in [SP-SEC-CommExt] Note 2: Usage of SSI between the SCS is not mandatory, but recommended. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec].

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.01 RE 1	Communication authentication	_ is implemented by: SP-SEC-CommExt-1.4-2: Each software process realizing an additional communication interface shall authenticate each communication partner (human user, other software process) by validating the partner's identity. Note: in case of certificate-based identification, see checks in chapter SP-SEC-CompSpec-5.5.3 - PKI certificate validation. In case of other identification, e.g. OpenID Connect / OAuth the checks for other identification schemes are applicable. _ is implemented by: SP-SEC-Comp-5.5.1-2: The Secure Component shall implement the mandatory interfaces defined in [SP-SEC-ServSpec] Table 1. It may need to implement additional optional interfaces defined in [SP-SEC-ServSpec]for its specified function or standard communication protocols defined in [SP-SEC-CommSpec]. Note 1: This ensures the identification, authentication, integrity, and confidentiality requirements, as well as the first step of authorisation for network based communication for interfaces defined in Shared Cybersecurity Services Specification. For all other communication interfaces, the requirements are listed in [SP-SEC-CommExt] Note 2: Usage of SSI between the SCS is not mandatory, but recommended. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec].

DRAFT

IEC 62443-4-2 CR 3.03	Security functionality verification	_ is implemented by: SP-SEC-Comp-5.7.2-1: The Secure Component supports the verification of the intended operation of security functions by the diagnostic values and maintenance methods in this chapter. Note: For SCS implementations, the functionality in the table below may be provided by existing secure administration interfaces instead of SSI-MNT.

Security Function	Verification	Verification time
Process Allowlisting	maintenance call `TestProcessIntegrityCheck()`	during normal operation
Security Logging	implicit tested via `TestProcessIntegrityCheck()` which produces a log message	during normal operation
Integrity checks	maintenance call `TestProcessIntegrityCheck()`	during normal operation
Certificates Management	maintenance nodes `InstalledTrustAnchors`, `InstalledCerts` and `RenewCert()`	during normal operation
Hardware trust anchor	only positive test case: maintenance nodes `InstalledTrustAnchors`, `InstalledCerts`	during normal operation
Host-based firewall	maintenance call `TestHostFirewall()`	during normal operation
Backup & Restore	calls to Backup & Restore interface (SSI-BKP)	during normal operation
Secure boot	only positive test case: Secure Component has successfully booted and reports **`SecurityStatus`**	during normal operation

DRAFT

Security Function	Verification	Verification time
Network Access control	only positive test case: Secure Component has successfully connected to the network and reports `SecurityStatus`	during normal operation
Identification and Authentication	any call to the maintenance interface involves user identification and authentication, testable using different users with different permissions	during normal operation
User Authorization	any call to the maintenance interface involves user authorization, testable using different users with different permissions	during normal operation
Random number generation	verification of using OS standard implementation for random number generation, check randomness for seeds after boot-up (esp. for components without a battery-buffered clock), check of entropy of random number generation	during product development
Electronic tamper detection	check detection when opening the encasing	during product development
Input validation	Fuzz testing	during product development
Deterministic output	Trigger a safe-state, document output settings	during product development
Hardware trust anchor	code review of section storing private keys	during product development
Secure Boot	Tamper firmware and reboot	during product development

DRAFT

Security Function	Verification	Verification time
Denial-of-service resilience	Create high network load	during product development and system / integration test
Hardware-related firmware update	Update hardware-related firmware	during product development and system / integration test
Network Access Control	negative test case: remove asset in SSI-IAM, trigger a reboot	during product development and system / integration test

DRAFT

IEC 62443-4-2 CR 3.03 RE 1	Security functionality verification during normal operation	_ is implemented by: SP-SEC-Comp-5.7.2-1: The Secure Component supports the verification of the intended operation of security functions by the diagnostic values and maintenance methods in this chapter. Note: For SCS implementations, the functionality in the table below may be provided by existing secure administration interfaces instead of SSI-MNT.

Security Function	Verification	Verification time
Process Allowlisting	maintenance call `TestProcessIntegrityCheck()`	during normal operation
Security Logging	implicit tested via `TestProcessIntegrityCheck()` which produces a log message	during normal operation
Integrity checks	maintenance call `TestProcessIntegrityCheck()`	during normal operation
Certificates Management	maintenance nodes `InstalledTrustAnchors`, `InstalledCerts` and `RenewCert()`	during normal operation
Hardware trust anchor	only positive test case: maintenance nodes `InstalledTrustAnchors`, `InstalledCerts`	during normal operation
Host-based firewall	maintenance call `TestHostFirewall()`	during normal operation
Backup & Restore	calls to Backup & Restore interface (SSI-BKP)	during normal operation
Secure boot	only positive test case: Secure Component has successfully booted and reports **`SecurityStatus`**	during normal operation

DRAFT

Security Function	Verification	Verification time
Network Access control	only positive test case: Secure Component has successfully connected to the network and reports `SecurityStatus`	during normal operation
Identification and Authentication	any call to the maintenance interface involves user identification and authentication, testable using different users with different permissions	during normal operation
User Authorization	any call to the maintenance interface involves user authorization, testable using different users with different permissions	during normal operation
Random number generation	verification of using OS standard implementation for random number generation, check randomness for seeds after boot-up (esp. for components without a battery-buffered clock), check of entropy of random number generation	during product development
Electronic tamper detection	check detection when opening the encasing	during product development
Input validation	Fuzz testing	during product development
Deterministic output	Trigger a safe-state, document output settings	during product development
Hardware trust anchor	code review of section storing private keys	during product development
Secure Boot	Tamper firmware and reboot	during product development

DRAFT

Security Function	Verification	Verification time
Denial-of-service resilience	Create high network load	during product development and system / integration test
Hardware-related firmware update	Update hardware-related firmware	during product development and system / integration test
Network Access Control	negative test case: remove asset in SSI-IAM, trigger a reboot	during product development and system / integration test

DRAFT

_ is implemented by: SP-SEC-Serv-12.6-1: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:SecurityFunctionalityVerification:TestProcessIntegrityCheck()`, which tests the functionality of the process integrity check.

Note: a typical implementation is to have an executable file with no functionality not in part of the process integrity check (e.g. an allowlist). This executable is still integrity protected, e.g. by secure boot. The executable is executed by this maintenance method. This triggers the process integrity check and issues a log message, which can be used to verify the security functionality of process allowlisting, security logs, time synchronization and real-time clock (time is part of a log message).

_ is implemented by: SP-SEC-Serv-12.6-2: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:SecurityFunctionalityVerification:TestHostFirewall()`, which tests the functionality of the host-based firewall.

Note: a typical implementation is to have a process try to open a connection when this maintenance method is called to the destination address, port and protocol (either UDP or TCP) and then terminates. In case the connection is blocked by the host-based firewall, a log message is issued.

		This can be used to verify the security functionality of the host-based firewall.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.04	Software and information integrity	_ is implemented by: SP-SEC-Comp-5.3.2-1: The Secure Component shall verify the integrity and authenticity of configuration data using the installed roots of trust before it is used. Note: configuration data is cryptographically signed. Verification of integrity and authenticity is done by verifying the signature. _ is implemented by: SP-SEC-Comp-5.2.5-1: The Secure Component shall use the Secure Boot functions defined by the used chipset manufacturer. _ is implemented by: SP-SEC-Comp-5.2.5-3: If a secure boot verification fails, the Secure Component should provide a visible or audible indication. Note: the visual or audible indication of an integrity check failure is recommended, as the Secure Component cannot securely log errors before successful start-up of the operating system. Examples could be a LED indication or audible notification. For COTS devices as PCs, laptops and servers, refer to manufacturer handbook for indications of a integrity failure during secure boot _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.04 RE 1	Authenticity of software and information	_ is implemented by: SP-SEC-Comp-5.3.2-1: The Secure Component shall verify the integrity and authenticity of configuration data using the installed roots of trust before it is used. Note: configuration data is cryptographically signed. Verification of integrity and authenticity is done by verifying the signature. _ is implemented by: SP-SEC-Comp-5.2.5-1: The Secure Component shall use the Secure Boot functions defined by the used chipset manufacturer. _ is implemented by: SP-SEC-Comp-5.2.5-3: If a secure boot verification fails, the Secure Component should provide a visible or audible indication. Note: the visual or audible indication of an integrity check failure is recommended, as the Secure Component cannot securely log errors before successful start-up of the operating system. Examples could be a LED indication or audible notification. For COTS devices as PCs, laptops and servers, refer to manufacturer handbook for indications of a integrity failure during secure boot _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.04 RE 2	Automated notification of integrity violations	_ is implemented by: SP-SEC-Comp-5.7.1-3: The Secure Component shall send log messages complying to the log message format defined in SP-SEC-ServSpec Ch 9.1 - Log Message Format Note: This ensures that the log messages contain the following data: a) timestamp (synchronized); b) source (originating device, software process or human user account); c) category; d) type; e) event ID; and f) event result _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).
IEC 62443-4-2 CR 3.05	Input validation	_ is implemented by: SP-SEC-Comp-5.3.4-1: The Secure Component shall validate the syntax, length and content of any input data. Note: specific care should be taken for input data received via external interfaces and from other sources (e.g. file systems). Examples for content checks are type checks and value range checks. The input checks are typically realized on the application layer which processes the input. A rule formulating input checks is to accept all data conforming to an interface spec and reject non-conforming data.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.06	Deterministic output	_ is implemented by: SP-SEC-Comp-5.3.5-1: If the Secure Component has physical I/O controlling an automation process, the Secure Component shall provide the capability to set all physical outputs to a predetermined state if normal operation cannot be maintained. Note: The predetermined state is normally the safe state of the component and normally invoked in fault situations and realized by the safety system.
IEC 62443-4-2 CR 3.07	Error handling	_ is implemented by: SP-SEC-Comp-5.7.1-1: The Secure Component shall send the logging events via SSI-LOG SP-SEC-ServSpec Ch 9 - LOG: Security Logging . Note: this ensures encryption of the log messages and ensures that no information is provided that can be exploited by adversaries to attack the system. _ is implemented by: SP-SEC-Serv-9-5: The communication partners using the SSI-LOG (log originator, log relay, log collector) shall use syslog over TLS as defined in RFC ~~SPPRAMSS-13763~~ - *Missing cross-reference* and ~~SPPRAMSS-13752~~ - *Missing cross-reference* for sending and/or receiving security log messages.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.08	Session integrity	_ is implemented by: : For resiliency, the operation of multiple time servers is recommended. _ is implemented by: SP-SEC-Serv-6.4-1: The SSI-PKI client shall provide the capability to request and rekey certificates using the CMP protocol version 2 via HTTP according to the Lightweight CMP Profile (LCMPP) ~~SPPRAMSS-13743~~ - *Missing cross-reference*. Note: Confidentiality protection is not needed because only public data is transferred. Since CMP includes integrity protection, an insecure transport protocol (HTTP in this case) can be used. _ is implemented by: SP-SEC-Serv-9-5: The communication partners using the SSI-LOG (log originator, log relay, log collector) shall use syslog over TLS as defined in RFC ~~SPPRAMSS-13763~~ - *Missing cross-reference* and ~~SPPRAMSS-13752~~ - *Missing cross-reference* for sending and/or receiving security log messages. _ is implemented by: SP-SEC-Serv-7-8: The SCS-IAM shall accept SCIM 2.0 requests via REST using HTTP over TLS according to ~~SPPRAMSS-13747~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-Serv-10-6: The SSI-UAS Endpoint shall implement single sign-on (SSO) based on OpenID Connect 1.0 (OIDC) as defined in ~~SPPRAMSS-13751~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-Comp-5.5.1-2: The Secure Component shall implement the mandatory interfaces defined in [SP-SEC-ServSpec] Table 1. It may need to implement additional optional interfaces defined in [SP-SEC-ServSpec]for its specified function or standard communication protocols defined in [SP-SEC-CommSpec]. Note 1: This ensures the identification, authentication, integrity, and confidentiality requirements, as well as the first step of authorisation for network based communication for interfaces defined in Shared Cybersecurity Services Specification. For all other communication interfaces, the requirements are listed in [SP-SEC-CommExt] Note 2: Usage of SSI between the SCS is not mandatory, but recommended. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec].

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 3.09	Protection of audit information	_ is implemented by: SP-SEC-Comp-5.7.1-1: The Secure Component shall send the logging events via SSI-LOG SP-SEC-ServSpec Ch 9 - LOG: Security Logging . Note: this ensures encryption of the log messages and ensures that no information is provided that can be exploited by adversaries to attack the system.
IEC 62443-4-2 CR 3.09 RE 1	Audit records on write-once media	_ is implemented by: : NOT IMPLEMENTED: **CR 3.9 RE 1**: Using hardware-enforced write-once media to store audit records. This SL4 requirement requires specialized hardware and does not provide a beneficial cost to security enhancement ratio. A more cost-effective solution to protect audit information from attackers is to install an isolated log server and connect it via a network tap (shadow logging) to the supervised network communication. This prevents an attacker to gain access to the shadow log server.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 4.1	Information confidentiality	_ is implemented by: SP-SEC-Comp-5.3.3-1: If read access authorisation to persistent data is required, the Secure Component shall encrypt this data. Note: this applies at least for all confidential data at rest. It could be realized using file system encryption which encrypts all persistent data. _ is implemented by: SP-SEC-Comp-5.5.1-2: The Secure Component shall implement the mandatory interfaces defined in [SP-SEC-ServSpec] Table 1. It may need to implement additional optional interfaces defined in [SP-SEC-ServSpec]for its specified function or standard communication protocols defined in [SP-SEC-CommSpec]. Note 1: This ensures the identification, authentication, integrity, and confidentiality requirements, as well as the first step of authorisation for network based communication for interfaces defined in Shared Cybersecurity Services Specification. For all other communication interfaces, the requirements are listed in [SP-SEC-CommExt] Note 2: Usage of SSI between the SCS is not mandatory, but recommended. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec]. _ is implemented by: SP-SEC-CommExt-1.5-2: If data in transit is considered confidential, a software process realizing an additional communication interface shall provide the capability to protect the confidentiality of data in transit. Note: this should, if applicable, be realized preferable using TLS with an encryption cipher. Examples of confidential data in transit are encryption keys, legally protected personal data, user credentials, person/user related data, financial information, security related logs and/or diagnosis data.
IEC 62443-4-2 CR 4.2	Information persistence	_ is implemented by: SP-SEC-Serv-12.5-1: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:ComponentLifecycleManagement:InitiateFactoryReset()`, which deletes persistent data to reset the component to factory state. Note 1: this method can be used as part of a decommissioning process Note 2: this method does not delete the factory key material (e.g. the MDC together with its root certificate will stay on the devices). Note 3: this methods provides the user with the ability to erase data which requires confidentiality protection from persistent memory.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 4.2 RE 1	Erase of shared memory resources	_ is implemented by: SP-SEC-Comp-5.1-2: The Secure Component shall use for implementation of security functionality proven or mature security libraries and security hardware. Note: proven/mature security libraries are widely and internationally used programming libraries. An example of a such security library is openSSL and operating system functions for obtaining random numbers. Using proven/mature security libraries limits implementation errors and risks of side-channel attacks, as well as purging of key material. Proven/mature security hardware refers to widely recognized and internationally used hardware components specifically designed for security purposes. Examples of standard security hardware include cryptographic modules certified under FIPS 140-2, tamper-resistant secure elements, and hardware security modules (HSMs),Trusted Platform Module (TPM) chips and CPUs with Trusted Execution Environments (TEE).
IEC 62443-4-2 CR 4.2 RE 2	Erase verification	_ is implemented by: SP-SEC-Serv-12.5-1: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:ComponentLifecycleManagement:InitiateFactoryReset()`, which deletes persistent data to reset the component to factory state. Note 1: this method can be used as part of a decommissioning process Note 2: this method does not delete the factory key material (e.g. the MDC together with its root certificate will stay on the devices). Note 3: this methods provides the user with the ability to erase data which requires confidentiality protection from persistent memory. _ is implemented by: SP-SEC-Comp-5.1-2: The Secure Component shall use for implementation of security functionality proven or mature security libraries and security hardware. Note: proven/mature security libraries are widely and internationally used programming libraries. An example of a such security library is openSSL and operating system functions for obtaining random numbers. Using proven/mature security libraries limits implementation errors and risks of side-channel attacks, as well as purging of key material. Proven/mature security hardware refers to widely recognized and internationally used hardware components specifically designed for security purposes. Examples of standard security hardware include cryptographic modules certified under FIPS 140-2, tamper-resistant secure elements, and hardware security modules (HSMs),Trusted Platform Module (TPM) chips and CPUs with Trusted Execution Environments (TEE).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 4.3	Use of cryptography	_ is implemented by: SP-SEC-COMM-3.1-5: The TLS endpoint shall support the cipher TLS_AES_256_GCM_SHA384. _ is implemented by: SP-SEC-COMM-3.1-6: The TLS endpoint shall support the cipher TLS_CHACHA20_POLY1305_SHA256. _ is implemented by: SP-SEC-COMM-3.1-7: If only integrity protection is required, the TLS endpoint shall support the cipher TLS_SHA384_SHA384. ~~SPPRAMSS-2034~~ - *Missing cross-reference* Note: Integrity-only protection can be used for Automatic Train Operation [Subset-148], Automatic Train Protection [Subset-037-3], and EULYNX SCI [Eu.Doc.92]. _ is implemented by: SP-SEC-Comp-5.3.2-1: The Secure Component shall verify the integrity and authenticity of configuration data using the installed roots of trust before it is used. Note: configuration data is cryptographically signed. Verification of integrity and authenticity is done by verifying the signature. _ is implemented by: SP-SEC-COMM-4-8: The OPC UA endpoint shall support the following Security Policies defined in UACore 1.05: • ECC-nistP256-ChaChaPoly (~~SPPRAMSS-18526~~ - *Missing cross-reference*) • ECC-nistP256-AesGcm (~~SPPRAMSS-18525~~ - *Missing cross-reference*) _ is implemented by: SP-SEC-COMM-5-7: The OPC UA endpoint shall support the Security Policy ECC-brainpoolP256r1 defined in Amendment 4: ECC for UACore 1.04 ~~SPPRAMSS-12392~~ - *Missing cross-reference* and in UACore 1.05 ~~SPPRAMSS-12386~~ - *Missing cross-reference*. _ is implemented by: SP-SEC-Comm-3.1-8: The TLS server shall reject ciphers not defined in this specification. _ is implemented by: SP-SEC-Comm-4-9: The OPC UA server shall reject Security Policies not defined in this specification.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 5.1	Network segmentation	_ is implemented by: SP-SEC-Comp-5.4.3-1: The Secure Component shall support to authenticate to the network using the SSI-NAC interface (refer to SP-SEC-ServSpec Ch 8 - NAC: Network Access Control). _ is implemented by: SP-SEC-Comp-5.4.1-2: The Secure Component can be capable to bind each communicating process to configured interface(s) corresponding to a specific VLAN. _ is implemented by: SP-SEC-Comp-5.4.1-3: The Secure Component can be capable to separate at least maintenance (e.g. SMI), diagnostic (e.g. SDI), security (e.g. SSI) and operational data (e.g. SCI) to specific VLANs. Note: There could be additional VLANS for example for further segmentation of SCI (different SIL level, different SSI-XXX), on-board specific VLANs. This further segmentation can be configured via the component configuration.
IEC 62443-4-2 CR 6.1	Audit log accessibility	_ is implemented by: SP-SEC-Serv-12.3-1: The SSI-MNT interface shall provide the maintenance method Security:GetSecurityLog(Time start, Time end) to access audit logs on a read-only basis for authorised humans and/or software processes. Note: The default method for log transmission is via SSI-LOG. This diagnostic method covers edge cases when log transmission was interrupted to retrieve local stored logs.
IEC 62443-4-2 CR 6.1 RE 1	Programmatic access to audit logs	_ is implemented by: SP-SEC-Serv-12.3-1: The SSI-MNT interface shall provide the maintenance method Security:GetSecurityLog(Time start, Time end) to access audit logs on a read-only basis for authorised humans and/or software processes. Note: The default method for log transmission is via SSI-LOG. This diagnostic method covers edge cases when log transmission was interrupted to retrieve local stored logs.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 6.2	Continuous monitoring	_ is implemented by: SP-SEC-Comp-5.7.1-1: The Secure Component shall send the logging events via SSI-LOG SP-SEC-ServSpec Ch 9 - LOG: Security Logging . Note: this ensures encryption of the log messages and ensures that no information is provided that can be exploited by adversaries to attack the system. _ is implemented by: SP-SEC-Serv-9.1.2-8: The log originator shall log at least the following events: a) access control; b) request errors; c) control system events; d) backup and restore event; e) configuration changes; and f) audit log events (incl. administrative actions, input validation errors) g) threats (attacks and probes) h) resource events (system resources reaching a threshold) i) availability (shutdown, failures, crashes).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 7.1	Denial of service protection	_ is implemented by: SP-SEC-Comp-5.4.4-2: After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally. Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds. This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1 _ is implemented by: SP-SEC-Comp-5.4.2-2: The host-based firewall shall deny by default all inbound and outbound connections except for the designed network communications of the Secure Component. _ is implemented by: SP-SEC-Comp-5.4.4-1: The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion. Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits.
IEC 62443-4-2 CR 7.1 RE 1	Manage communication loads	_ is implemented by: SP-SEC-Comp-5.4.4-3: The Secure Component shall provide the capability to only allow a configurable maximum number of concurrent sessions per interface for any given user (human, or technical user). _ is implemented by: SP-SEC-Comp-5.4.4-2: After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally. Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds. This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1
IEC 62443-4-2 CR 7.2	Resource management	_ is implemented by: SP-SEC-Comp-5.4.4-1: The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion. Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 7.3	Control system backup	_ is implemented by: SP-SEC-Comp-5.6.3-1: If operational data is not part of the configuration data from [I-STD-MAINTENANCE - SMI] interface, the Secure Component shall backup operational data which is relevant for its operational availability via SSI-BKP SP-SEC-Serv - Ch. 11 - BKP: Backup and Restore Note 1: Backups are intended for operational data that is relevant for operational availability (e.g. changes in databases), but is not part of the configuration (e.g. obtained via I-STD-MAINTENANCE (SMI)). Most rail automation devices receive all data required for operational data via I-STD-MAINTENANCE and do not need the interface SSI-BKP Note 2: Backups are triggered remotely via SSI-BKP, additionally the Secure Component has also the option to trigger a backup creation locally , e.g. based on time or change events.
IEC 62443-4-2 CR 7.3 RE 1	Backup integrity verification	_ is implemented by: SP-SEC-Comp-5.6.3-3: If the Secure Component backups operational data, the Secure Component shall be capable of verifying the authenticity and integrity of backup data received via SSI-BKP SP-SEC-ServSpec Ch 11 - BKP: Backup and Restore
IEC 62443-4-2 CR 7.4	Control system recovery and reconstitution	_ is implemented by: SP-SEC-Comp-5.6.1-1: The Secure Component shall support the update of software and configuration via the interface [I-STD-MAINTENANCE - SMI] . Note 1: when updating non-safety related software, typically also the process allowlist has to be updated. Note 2: this supports together with the backup and restore functionality (chapter 5.6.3) the recovery and reconstitution to a known secure state after a disruption or failure. _ is implemented by: SP-SEC-Comp-5.6.3-2: If the Secure Component backups operational data , the Secure Component shall be capable of restoring operational data via SSI-BKP SP-SEC-ServSpec Ch 11 - BKP: Backup and Restore
IEC 62443-4-2 CR 7.6	Network and security configuration settings	_ is implemented by: SP-SEC-Serv-12.4-2: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:ComponentConfiguration:GetNetworkConfiguration()`, which returns a JSON file including all configuration file names with the SHA-256 hash of the file content Note: this maintenance method can be used to detect changes in network configuration by comparing the result with previously stored configurations (or hashes). _ is implemented by: : The Secure Component shall implement the SSI-MNT interface defined in SP-Sec-Serv Ch. 12. Note: the Secure Component acts as an OPC UA maintenance server.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 7.6 RE 1	Machine-readable reporting of current security settings	_ is implemented by: SP-SEC-Serv-12.4-2: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:ComponentConfiguration:GetNetworkConfiguration()`, which returns a JSON file including all configuration file names with the SHA-256 hash of the file content Note: this maintenance method can be used to detect changes in network configuration by comparing the result with previously stored configurations (or hashes). _ is implemented by: : The Secure Component shall implement the SSI-MNT interface defined in SP-Sec-Serv Ch. 12. Note: the Secure Component acts as an OPC UA maintenance server.
IEC 62443-4-2 CR 7.7	Least functionality	_ is implemented by: SP-SEC-Comp-5.3.6-1: The Secure Component shall enable only required and documented functions and services and their corresponding exposed ports and protocols. Note: Examples for possible unused functions and services are email, voice over IP, instant messaging, and file transfer protocol (FTP). This requirement can be verfied by external port scans (no difference between documented required ports and detected ports). When using standard OS and applications, OS and application hardenening can be an essential measure to fulfill this requirement. Hardening can be demonstrated by a relevant **[CIS benchmark]**, achieving compliance to at least Level 1 or in accordance with a comparable benchmark and compliance level.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 CR 7.8	Control system component inventory	_ is implemented by: SP-SEC-Comp-5.5.4-2: The Secure Component shall contain the following configuration items before starting the commissioning process : • IP-Address or FQDN of SCS-PKI • IP-Address or FQDN of SCS-STS • IP-Address or FQDN of SCS-IAM • Operator Trust Anchor • Identifiers required for operator certificate requests (e.g. EULYNX identifier) Note: For initial provisioning of software and configuration initially the address of the update/config server (e.g. MDM) is required. Configuration items are defined in SP-SEC-Comp-6.2-2 Configuration items _ is implemented by: SP-SEC-Serv-12.2-3: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:TrustStore:InstalledCerts:GenerateFileForRead()`, which creates a single tar archive with one pem file for every leaf certificate installed on the Secure Component including the full certificate chain. _ is implemented by: SP-SEC-Serv-12.4-1: The SSI-MNT interface shall provide the maintenance method `SSI-MNT:ComponentConfiguration:GetComponentConfiguration()`, which returns a JSON file including all configuration file names with the SHA-256 hash of the file contentNote: this maintenance method can be used to detect changes in component configuration by comparing the result with previously stored configurations (or hashes). _ is implemented by: : The Secure Component shall implement the SSI-MNT interface defined in SP-Sec-Serv Ch. 12. Note: the Secure Component acts as an OPC UA maintenance server.
IEC 62443-4-2 EDR/HDR/ NDR 2.13	Use of physical diagnostic and test interfaces	_ is implemented by: SP-SEC-Comp-5.2.9-1: If physical diagnostic and test interfaces are accessible without opening the protected enclosure, the Secure Component shall disable physical factory diagnostic and test interfaces during manufacturing or commissioning.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 EDR/HDR/ NDR 2.13 RE 1	Active monitoring	_ is implemented by: : NOT IMPLEMENTED: **EDR/NDR/HDR 2.13 RE1**: Active monitoring of physical factory diagnostic and test interfaces if they are disabled, creation of a log for access attempts. Monitoring these interfaces (e.g. JTAG) does not provide additional security (since there are numerous other attacks when the attacker has physical access to the component, e.g. installing own probes).
IEC 62443-4-2 EDR/HDR/ NDR 3.10	Support for updates	_ is implemented by: SP-SEC-Comp-5.6.1-1: The Secure Component shall support the update of software and configuration via the interface [I-STD-MAINTENANCE - SMI] . Note 1: when updating non-safety related software, typically also the process allowlist has to be updated. Note 2: this supports together with the backup and restore functionality (chapter 5.6.3) the recovery and reconstitution to a known secure state after a disruption or failure.
IEC 62443-4-2 EDR/HDR/ NDR 3.10 RE 1	Update authenticity and integrity	_ is implemented by: SP-SEC-Comp-5.6.1-3: The Secure Component shall verify the signature of the update packages using the corresponding installed roots of trust before installation.
IEC 62443-4-2 EDR/HDR/ NDR 3.11	Physical tamper resistance and detection	_ is implemented by: SP-SEC-Comp-5.2.6-1: When powered, the Secure Component or its installation encasing shall provide a tamper detection mechanism which detects the opening of the physical encasing. Note: A typical installation encasing is a cabinet.
IEC 62443-4-2 EDR/HDR/ NDR 3.11 RE 1	Notification of a tampering attempt	_ is implemented by: SP-SEC-Comp-5.2.6-2: If tampering is detected and the Secure Component implements tamper detection, the Secure Component shall provide notification of the detection to the SSI-LOG service.
IEC 62443-4-2 EDR/HDR/ NDR 3.12	Provisioning product supplier roots of trust	_ is implemented by: SP-SEC-Comp-6.1-1: Before commissioning the Secure Component shall retrieve and store its Manufacturer Device Certificate (MDC) and the corresponding manufacturer root CA certificate. Note: the Manufacturer Device Certificate (MDC) plays a role in the commissioning identification/authentication/security bootstrapping process, and software/firmware updates.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 EDR/HDR/ NDR 3.13	Provisioning asset owner roots of trust	_ is implemented by: SP-SEC-Comp-5.5.4-8: If at least one valid operator trust anchor has been installed, the Secure Component shall support installation and update of operator trust anchors contained in a trust anchor bundle, where the trust anchor bundle is signed using the private key corresponding to a trusted Operator Trust Anchor Signer Certificate (OTASC). Note: An OTASC is considered trusted if it was provisioned through a previously accepted MTASC-signed trust anchor bundle or if its certification path terminates at a trusted operator root CA certificate. _ is implemented by: SP-SEC-Comp-5.5.4-7: If no valid operator trust anchor is installed, the Secure Component shall support installation of operator trust anchors contained in a trust anchor bundle, where the trust anchor bundle is signed using the private key corresponding to the Manufacturer Trust Anchor Signer Certificate (MTASC). Note: The operator explicitly identifies the certificates designated as trust anchors within the trust anchor bundle. The trust anchor bundle may additionally contain associated CRLs and metadata, such as a bundle version number or sequence number for rollback protection.
IEC 62443-4-2 EDR/HDR/ NDR 3.14	Integrity of the boot process	_ is implemented by: SP-SEC-Comp-5.2.5-1: The Secure Component shall use the Secure Boot functions defined by the used chipset manufacturer. _ is implemented by: SP-SEC-Comp-5.2.5-5: The Secure Component shall continue with the next boot stage only if the integrity and authenticity checks are successful. _ is implemented by: SP-SEC-Comp-5.2.5-6: The Secure Component shall verify all secure boot stages from start of the hardware to the operating system / root file system. Note: Examples of secure boot stages are chipsets, BIOS/UEFI, boot loader, operating system and other static code/applications on the file system.
IEC 62443-4-2 EDR/HDR/ NDR 3.14 RE 1	Authenticity of the boot process	_ is implemented by: SP-SEC-Comp-5.2.5-2: The Secure Component shall verify the authenticity of the firmware, bootloader, and operating system using trusted public keys or certificate chains managed by the manufacturer.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 HDR 3.02 RE 1	Report version of code protection	_ is implemented by: : NOT IMPLEMENTED: **HDR 3.2 RE 1**: Reporting the version of software and files for code protection only is applicable for anti-virus solution, which is not advised to use in automation products for protection against malware. This specification uses a runtime-integrity checks for software processes to protect against the execution unauthorised software. See SP-SEC-CompSpec Ch 5.3.1 Process runtime-integrity check
IEC 62443-4-2 NDR 1.06	Wireless access management	_ is implemented by: SP-SEC-Comp-7.1.4-1: If a Network Component supports wireless access management (e.g. WLAN access point), the Network Component shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication with a control system. Note: this can be achieved using IEEE 802.1x EAP TLS.
IEC 62443-4-2 NDR 1.06 RE 1	Unique identification and authentication	_ is implemented by: SP-SEC-Comp-7.1.4-1: If a Network Component supports wireless access management (e.g. WLAN access point), the Network Component shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication with a control system. Note: this can be achieved using IEEE 802.1x EAP TLS.
IEC 62443-4-2 NDR 1.13	Access via untrusted networks	_ is implemented by: SP-SEC-Comp-7.1.2-1: If the Network Component provides access from untrusted networks, the Network Component shall control and monitor the access.
IEC 62443-4-2 NDR 1.13 RE 1	Explicit access request approval	_ is implemented by: SP-SEC-Comp-7.1.2-2: If the Network Component provides access from untrusted networks, the Network Component shall be capable of denying access via untrusted networks unless explicitly approved by an assigned role.
IEC 62443-4-2 NDR 5.2	Zone boundary protection	_ is implemented by: SP-SEC-Comp-7.1.3-1: The Network Component implementing a firewall shall be capable of deny-all and allow-on-exception filter configuration (allowlist configuration).
IEC 62443-4-2 NDR 5.2 RE 1	Deny by default, permit by exception	_ is implemented by: SP-SEC-Comp-7.1.3-1: The Network Component implementing a firewall shall be capable of deny-all and allow-on-exception filter configuration (allowlist configuration).

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 NDR 5.2 RE 2	Island mode	_ is implemented by: SP-SEC-Comp-7.1.3-3: The Network Component at a zone boundary implementing a firewall shall be capable of enabling an island mode. Note: island mode is defined as blocking or disabling interfaces to another network zone (e.g. from signalling network to back-office or enterprise network)
IEC 62443-4-2 NDR 5.2 RE 3	Fail close	_ is implemented by: SP-SEC-Comp-7.1.3-4: The Network Component at a zone boundary implementing a firewall shall automatically block connections (fail close) during a failure of the network filter mechanisms.
IEC 62443-4-2 NDR 5.3	General purpose person-to-person communication restrictions	_ is implemented by: SP-SEC-Comp-7.1.3-1: The Network Component implementing a firewall shall be capable of deny-all and allow-on-exception filter configuration (allowlist configuration). _ is implemented by: SP-SEC-Comp-7.1.3-2: The Network Component implementing a firewall shall be capable of packet filtering according to source and destination port, source and destination addresses and direction of flow.
IEC 62443-4-2 SAR/EDR/ HDR/NDR 2.04	Mobile code	_ is implemented by: SP-SEC-Comp-5.3.1-1: The Secure Component shall only start a software process if it passes the runtime integrity check. Note: This protects against execution of unauthorised software. Typical solutions are a process allowlist or anomaly detection. An allowlist typically contains the hashes of the authorised executable binaries.
IEC 62443-4-2 SAR/EDR/ HDR/NDR 2.04 RE 1	Mobile code integrity check	_ is implemented by: SP-SEC-Comp-5.6.1-3: The Secure Component shall verify the signature of the update packages using the corresponding installed roots of trust before installation. _ is implemented by: SP-SEC-Comp-5.6.1-4: The Secure Component shall reject update packages without a valid signature.

DRAFT

IEC 62443 4-2	Requirement	implemented by
IEC 62443-4-2 SAR/EDR/ HDR/NDR 3.02	Protection from malicious code	_ is implemented by: SP-SEC-Comp-5.6.1-3: The Secure Component shall verify the signature of the update packages using the corresponding installed roots of trust before installation. _ is implemented by: SP-SEC-Comp-5.3.1-1: The Secure Component shall only start a software process if it passes the runtime integrity check. Note: This protects against execution of unauthorised software. Typical solutions are a process allowlist or anomaly detection. An allowlist typically contains the hashes of the authorised executable binaries.
97 items found		

4.3 CLC/TS 50701 compliance

Table containing tracing of the requirements for a Zone Description (CLC/TS 50701 6.4.1) and Cybersecurity Requirements Specification (CRS), see chapter CLC/TS 50701 7.2.10.

DRAFT

TS 50701 - 6.4.1-1a	Risk of the assets, in terms of Integrity, Availability and Confidentiality	_ is implemented by: SP-SEC-Comp-4.2.4.6-1: The main risks for the asset in the Zone-SC (the Secure Component) is a compromise of the following protection objectives: 1. Integrity: can lead to loss of control, loss of safety, loss of essential functions 2. Availability: can lead to loss of control, loss of operation 3. Confidentiality: can lead to attacks on integrity and availability when confidential key material is extracted (impersonating attack) Note: a detailed list of threats is described in [SP-SEC-ThreatCat].

DRAFT

TS 50701 - 6.4.1-1b	Type of interfaces or connection to the other parts of the SuC (e.g. wireless)	_ is implemented by: SP-SEC-Comp-4.2.4.5-2: The table below describes the logical and physical access points for each conduit.

Conduit	Logical access point	Physical access point	Data flows	Connected zone
Interface to an adjacent Secure Component	Secure Component (e.g SCI endpoint)	Ethernet / Fibre port or radio (GSM-R, FRMCS, 5G)	mainly Safety-related communication, in some cases non-safety related communication	adjacent Secure Component zone
Interface to Shared Cybersecurity Services and OT Shared Security Services	Secure Component (SMI, SDI, SSI endpoints)	Ethernet / Fibre port or radio (GSM-R, FRMCS, 5G)	SMI messages, SDI messages, SSI messages	OT service zone
Additional Interfaces to other components/ services	Secure Component (other endpoint)	Ethernet / Fibre port or radio (GSM-R, FRMCS, 5G)	other communication specific	adjacent Secure Component, OT service zone

_ is implemented by: SP-SEC-DocTempl-5-8: <description of all logical interfaces / communication matrix (protocols, port numbers used, physical port used, type of data transmitted, interfacing partners)>

_ is implemented by: SP-SEC-DocTempl-5-7: <documented physical interfaces using photos, schematics and/or wiring schematics>

DRAFT

TS 50701	Requirement	implemented by
TS 50701 - 6.4.1-1c	Physical or logical location	_ is implemented by: SP-SEC-Comp-4.2.4.3-1: The physical boundary of the Zone-SC in context of this specification is the encasing of the Secure Component. Note: Further physical boundaries may exists in the environment (rack, cabinet, room) or inside the Secure Component (composed devices, e.g. host with virtual machine).
TS 50701 - 6.4.1-1d	Access requirements	_ is implemented by: SP-SEC-CommExt-1.4-4: Each software process realizing an additional communication interface shall enforce access based on retrieved permissions. Note: in cases of no network availability or no access to an IAM service instance, the implementation should fall back on a default or configurable permission list residing on the component. _ is implemented by: SP-SEC-Comp-5.5.1-1: If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec].
TS 50701 - 6.4.1-1e	Operational function	_ is implemented by: SP-SEC-Comp-4.1.2-1: A Secure Component implements one or more control functions of a rail system. The intended function is automatic control or manual control combined with operator view.
TS 50701 - 6.4.1-1f	Organization responsibilities for each asset	_ is implemented by: SP-SEC-Comp-4.2.4.2-1: The accountable organisation for the Zone-SC is the railway duty holder. For trackside and centrally installed Secure Components this can be the infrastructure manager, for Secure Components installed on rolling stock the vehicle owner.
TS 50701 - 6.4.1-1g	Safety aspect	_ is implemented by: SP-SEC-Comp-4.2.4.4-1: Secure Components implementing safety-related functions for the rail system have a safety designation up to SIL4.

DRAFT

TS 50701	Requirement	implemented by
TS 50701 - 6.4.1-1h	Technology lifecycle, e.g. product lifecycle, obsolescence.	_ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>
TS 50701 - 7.2.10b	List of detailed security requirements, including SL-T, assumptions and security...	_ is implemented by: SP-SEC-Comp-5: List of Detailed Security Requirements
TS 50701 - 7.2.10c	SuC description (see 6.2)	_ is implemented by: SP-SEC-Comp-4.1.1: SuC Scope and Boundary
TS 50701 - 7.2.10d	Zone or conduit drawings (see 6.4)	_ is implemented by: SP-SEC-Comp-4.2.3: Zone and Conduits Drawing
TS 50701 - 7.2.10e	Zone or conduit characteristics (see 6.4)	_ is implemented by: SP-SEC-Comp-4.2.4: Zone and Conduits Characteristics
TS 50701 - 7.2.10f	Operating environment assumptions (see 6.2 and 7.2.4.4.3)	_ is implemented by: SP-SEC-Comp-4.2.5: Operating Environment Assumptions _ is implemented by: SP-SEC-DocTempl-5-9: <typical network architecture diagram and/or system architecture diagrams depicted the Secure Component in the system context>

DRAFT

TS 50701	Requirement	implemented by
TS 50701 - 7.2.10g	Threat environment (see 6.2 and 7.2.1)	_ is implemented by: SP-SEC-Comp-4.2.6-1: The following attacker types are considered from threat and risk analysis: state agency, criminal organization and internal attacker. This includes the cybersecurity threats from terrorists, hacktivists and script kiddies. _ is implemented by: SP-SEC-Comp-4.2.6-2: The threats considered for this specification are described in the [SP-SEC-ThreatCat].
TS 50701 - 7.2.10h	Risk Acceptance (see 6.5.3)	_ is implemented by: SP-SEC-Comp-8: Residual risk
TS 50701 - 7.2.10i	Regulatory requirements	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Regulatory Compliance Tracing, v1.1
TS 50701 - 7.2.10k	Cybersecurity requirements and security-related application conditions shall be...	_ is implemented by: SP-SEC-Comp-8: Residual risk
TS 50701 - 7.2.10l	For requirement tracing, cybersecurity requirements that are necessary to protec...	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Support for essential functions, v1.1
18 items found		

DRAFT

4.4 IEC PT 63452 compliance

Table containing IEC 63452 CDV req no, title and corresponding req or chapter to the SP Cybersecurity specifications.

IEC 63452	Topic	Requirement	implemented by
IEC 63452 SO-01-01	Identification of the railway system	The railway duty holder shall identify and document the scope of its railway system and railway applications, identifying OT systems , and segregating them from IT systems. The railway duty holder shall, where no clear assignment to IT or OT is apparent, decide if the system is to be considered as IT or OT.	_ is implemented by: SP-SEC-Comp-4.1: General SuC Description
IEC 63452 SO-02-01	Definition of a high-level railway system model	The railway duty holder shall establish and maintain a high-level system model of the railway system that identifies subsystems grouped according to criteria such as location, functionality, or organizational context.	_ is implemented by: SP-SEC-Comp-4.1.2: High-level Description
IEC 63452 SO-03-01	Definition of a high-level railway zone model	The railway duty holder shall establish and maintain a high-level zone model of the railway system.	_ is implemented by: SP-SEC-Comp-4.1.2: High-level Description

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 SO-04-01	Specification of shared cybersecurity services	The railway duty holder shall define which shared cybersecurity services are part of the railway system.	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.1
IEC 63452 CP-01-01	Railway OT cybersecurity policy	The railway duty holder shall establish and maintain a railway OT cybersecurity policy that: • includes the high-level objectives and challenges of the organization for securing the railway system, • is aligned with the overall cybersecurity policy of the organization, • is approved by management	_ is implemented by: SP-SEC-Pgrm-5-1: The railways shall implement an ISMS based on ISO 27001, chapter 4.4.

DRAFT

IEC 63452 CP-01-02	Railway OT Cybersecurity Programme(s)	The asset owner shall establish and maintain a railway OT cybersecurity programme for each of its railway applications. A railway OT cybersecurity programme shall be aligned with the railway OT cybersecurity policy, and shall cover cybersecurity aspects of at least the following topics: a) Scope b) Information sharing management c) Competency management d) Inventory management e) Supply chain management f) Risk management g) Business continuity management h) Operations and maintenance management i) Vulnerability management j) Patch management k) Incident management l) Cybersecurity monitoring m) Continuous cybersecurity assurance including Cybersecurity case update n) Decommissioning management o) Data protection management	_ is implemented by: SP-SEC-Pgrm-5-1: The railways shall implement an ISMS based on ISO 27001, chapter 4.4. _ is implemented by: SP-SEC-Pgrm-5-10: The railway shall establish a security awareness and training program based on ISO 27002 chapter 6.3. _ is implemented by: SP-SEC-Pgrm-5-7: The railway shall define roles and responsibilities based on ISO 27002, chapter 5.2. _ is implemented by: 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 _ is implemented by: 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. _ is implemented by: 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 Secure Component based on ISO 27002 chapter 8.8. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9.2-1: The railway shall document the decommissioning process.

DRAFT

			_ is implemented by: 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. _ is implemented by: P-SEC-Pgrm-12.1-3: The railway shall have a continuity management based on ISO 27002 5.30 _ is implemented by: SP-SEC-Pgrm-5-21: The railway shall implement review processes for it's ISMS based on ISO 27001 chapters 9 and 10.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CP-02-01	Information sharing management	The asset owner shall establish, maintain, and apply an information sharing management process. This process shall include: a) Confidentiality management for sharing technical information between stakeholders through the supply chain and for each phase of life-cycle (from tender to decommissioning) b) Confidentiality management for sharing sensitive information directly linked to cybersecurity aspects (e.g. on secrets, vulnerabilities) c) Incident process to mitigate leak of data The information sharing management process shall comply with applicable relevant legislation (e.g.: personal data).	_ is implemented by: 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. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-11-13: The railway shall define an incident handling and response process based on ISO 27002 chapter 5.26.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CP-03-01	Competency management	This requirement applies to Asset Owner, System Integrator, Maintenance Service Provider. The organization shall establish and maintain a cybersecurity competency management process to ensure the cybersecurity competencies of personnel participating in the life-cycle of the railway application, according to their role and responsibilities. The process shall include: a) identification of cybersecurity roles and responsibilities and their associated skills. b) periodic evaluation of people current competencies versus the ones requested by their role (competency gap) c) delivering of the training / awareness programs to achieve the required competencies	_ is implemented by: SP-SEC-Pgrm-5-11: The railway shall establish security responsibilities training according to IEC 62443-2-1 Org 1.5. _ is implemented by: SP-SEC-Pgrm-10-19: The railway shall define roles following the segregation of duties principle.
IEC 63452 CP-04-01	Inventory management	The asset owner shall establish and maintain the process to identify the current and historical baseline of the railway assets and make sure the correctness of any change to baselines.	_ is implemented by: 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. _ is implemented by: 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.

DRAFT

IEC 63452 CP-05-01	Supply chain management	This requirement applies primary to the organisation for Asset Owner, System Integrator, Maintenance Service Provider. The organization shall establish and maintain a management processes to address their supply chain risks throughout the cybersecurity life-cycle. This management process shall ensure: a) Clear identification of the delegated cybersecurity tasks including the scope of work and the relationship between acquirer and its suppliers along the cybersecurity life-cycle b) Identification of relevant cybersecurity criteria applicable to the supplier selection process and to the supplier evaluation process c) Identification of the cybersecurity requirements for suppliers, from both technical and management process perspectives d) Continuous monitoring of suppliers including the improvement action plan for suppliers.	_ is implemented by: SP-SEC-Pgrm-5.1-3: The railway shall include security requirements in the supplier qualification process based on ISO 27002 chapter 5.19. _ is implemented by: 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. _ is implemented by: 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. _ is implemented by: v: The railway shall define requirements for the availability of spare parts considering security related disturbances in the supply chain. _ is implemented by: 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)] _ is implemented by: SP-SEC-Pgrm-5.1-1: The railway shall implement supply chain security management based on ISO 27002 5.21. _ is implemented by: SP-SEC-Pgrm-13.2-2: The supplier shall implement supply chain security management. Note: Recommended activities for supply chain management are

DRAFT

			document in IEC 62443-4-1 (SM-9, SM-10) and ISO 27002 5.21.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CP-06-01	Risk management	The asset owner shall establish and maintain a risk management process to identify and address the cybersecurity risks related to its railway system. This shall include a) Identification of the threats, vulnerabilities, and risks related to its railway applications, b) Risk acceptance criteria and risk matrices to decide level of likelihood, impact, risk, c) Procedure to document and keep track of the identified risks in a risk register - to establish the plan of risk treatment in line with the risk register, d) Follow-up of the execution of the risk treatment plan until its closure.	_ is implemented by: SP-SEC-Pgrm-5-1: The railways shall implement an ISMS based on ISO 27001, chapter 4.4.
IEC 63452 CP-07-01	Business continuity management	The railway duty holder shall include disruption of train operation in the scope of their business continuity management plan in cybersecurity aspect. This plan shall include a clear, accessible, step-by-step recovery procedure to restore the proper operation of the railway system within a targeted time-frame.	_ is implemented by: 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.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CP-08-01	Data Protection Management	The asset owner shall establish, maintain a data management processes to consider the protection of the railway applications sensitive data throughout the entire lifecycle. This management processes shall include, a) Identification and classification of data with the criticality level of confidentiality b) Identification of ownership for sensitive data - Definition of the minimum retention time for the sensitive data c) Definition of account to be able to access for each sensitive data d) Method and safeguard of protecting sensitive data including encryption key management e) Logging for generation, transfer/store, use, update and disposal of sensitive data f) Incident response procedure in case of disclosure or compromise of sensitive data	_ is implemented by: SP-SEC-Pgrm-9-4: The railway shall have policies and procedures related to data retention based on ISO 27002 5.33. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9-2: The railway shall use the Traffic Light Protocol (TLP) 2.0 for classifying information. _ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9-8: The railway shall implement IEC 62443-2-1 Data 1.7. _ is implemented by: SP-SEC-Pgrm-9-7: The railway shall implement IEC 62443-2-1 Data 1.5.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 LC-01-01	Assign Project Cybersecurity Manager	The asset owner, the system integrator and the maintenance service provider shall each respectively assign a project cybersecurity manager as the single point of contact for their respective organisations and responsible for the cybersecurity of the delivered or maintained railway solution/application. The project cybersecurity managers within their respective organizations shall monitor all cybersecurity activities for which they are responsible throughout the entire lifecycle.	

DRAFT

IEC 63452 LC-02-01	Plan project cybersecurity activities	Each organisation involved in the railway application lifecycle shall plan and document its cybersecurity activities according to its role, by identifying the applicable requirements from Clause 6 to Clause 9 of this document. All requirements from Clause 6 to Clause 9 shall be allocated to at least one of the involved organisations. An organization that has more than one role (AO, SI, MSP) may have a single cybersecurity management plan covering all its cybersecurity activities. The plans shall identify responsibilities for planned activities. Where responsibilities are shared with other stakeholders, confirmation shall be provided that these stakeholders have accepted their co-responsibilities. The cybersecurity management plans shall define the cybersecurity roles and responsibilities, organization, and activities to be carried out during each phase of the applied lifecycle. The following aspects shall be defined for each of these activities: a) objective b) dependencies on other activities c) assumptions d) deliverables to be produced e) link with the phases of the life cycle used for the railway	

DRAFT

		solution. The cybersecurity management plans shall consider all cybersecurity activities and deliverables listed in 6.4 applicable to the asset owner or system integrator respectively. For minor projects (e.g. modification of a component with the same functionalities, interfaces and cybersecurity capabilities; small enhancements with limited cybersecurity impact for an existing railway application), some activities of Clauses 6 to 9 may be skipped or optimised (e.g. no formal approval or handover plan when the AO takes over the roles from the ISP or MSP). The accountability of these will be with asset owner. Typically, these optimisations could be supported by a pre-defined zone model, an acceptance of the IRA, or a reference system. In all the other cases, any exception shall be justified by a security analysis, under the accountability of the asset owner. In the railway sector, the lifecycle given in IEC 62278-1 is typically used, but different lifecycles may be used as long as all the cybersecurity activities presented in Table 4 are performed, associated deliverables are produced and mapping between activities and lifecycle phases is provided.	

DRAFT

		The asset owner shall approve the cybersecurity management plan of the other organizations involved, if any.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 LC-0x-0x	Requirements for ISP security program	The asset owner shall establish the requirements for the expected capabilities and constraints **according to IEC62443-2-4** of the ISP/MSP security programs. NOTE The ** part is only necessary if we consider we shall refer to IEC62443-4-2 in the requirements, otherwise, we can skip it.	
IEC 63452 LC-02-02	Security issues during design phase	The system integrator shall specify and document in the cybersecurity management plan the process for addressing the following cybersecurity management aspects prior to the handover of the railway solution,: - vulnerability management, - patch management, - risk management, - cybersecurity monitoring, - incident management.	
IEC 63452 LC-03-01	Manage interaction with safety teams	The system integrator's project cybersecurity management plan shall document the interaction between the safety and cybersecurity teams throughout the development of the railway solution, identifying the synchronization points and the deliverable to be reviewed in each case. The cybersecurity case shall be communicated to the system integrator's safety team.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 LC-04-01	Cybersecurity requirement traceability	The system integrator shall ensure that cybersecurity requirements are systematically identified and have complete and correct traceability throughout the railway solution development life cycle up to the handover.	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Regulatory Compliance Tracing, v1.1
IEC 63452 ZR-01-01	Identify the SUC, its security perimeter and access points	The asset owner shall identify the SUC, including its essential functions, the demarcation of the security perimeter and the identification of all access points to the SUC.	_ is implemented by: : SP-SEC-SYS_DESC-5: Interfaces / Access Points _ is implemented by: SP-SEC-SYS_DESC-2: Scope and Boundary _ is implemented by: SP-SEC-SYS_DESC-2.2: Essential Functions
IEC 63452 ZR-01-01	Identify the cybersecurity context	The asset owner shall define the cybersecurity context applicable to the SUC: – threat environment – cybersecurity risk acceptance criteria – operational environment assumptions	_ is implemented by: SP-SEC-Comp-4.2.6: Threat Environment _ is implemented by: SP-SEC-Comp-4.2.5: Operating Environment Assumptions _ is implemented by: SP-SEC-Comp-4.2: Component Security Context

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-02-01	Initial risk assessment	The appointed organization, according to the Cybersecurity Management Plan, shall perform an initial risk assessment on the SUC or confirm that a previous initial risk assessment is still applicable. The initial risk assessment shall identify the worst-case unmitigated cybersecurity risks that could result from the interference with, breach, disruption of or disablement of the SUC's operation. The result of the analysis shall be documented in the risk assessment report.	_ is implemented by: SP-SEC-Comp-4.2.7-1: The initial risk analysis is documented in [SP-SEC-ThreatAna]

DRAFT

IEC 63452 ZR-03-01	Partitioning of the SUC	The appointed organization, according to the Cybersecurity Management Plan, shall establish the zones and conduits of the SUC. The assets shall be grouped to security zones that are connected by conduits, based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization. The following rules shall be used for grouping assets to zones: a) Business assets are separated from control assets, into different zones; b) Safety-related assets are grouped into dedicated zones which are logically or physically separated from zones with non-safety-related assets; c) Temporarily connected devices are grouped into separate zones from permanently connected devices; d) Wireless connected devices are grouped into separate zones from wired devices; e) Devices permitted to make connections to the SUC remotely via external networks are grouped into a separate zone or zones; f) Security devices are located at the zone boundary, protecting the zone; g) Assets belonging to an OT cloud (e.g. Cloud application) are grouped into a separate zone or zones. Exceptions (eg: due to architecture constraints) to the above rules shall be justified in the risk assessment report.	_ is implemented by: SP-SEC-Comp-4.2.3-2: Generic Security Zoning <Image: diagram_20240922-1629.25191.mxg.svg> *Figure 1 Generic Security Zoning*

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-04-01	Compare initial risk with tolerable risk	The appointed organization, according to the Cybersecurity Management Plan, shall compare the initial risk determined in ZR-02-01 (see 7.4.4) to the Asset Owner's tolerable risk defined for the SUC (see cybersecurity context, including Risk acceptance criteria from ZR-01-02 in 7.3.5). If the initial risk exceeds the tolerable risk, the System Integrator shall perform a detailed risk assessment as defined in ZR-05-01 (see 7.7.4). The results of this comparison shall be documented into the risk assessment report.	_ is implemented by: SP-SEC-DRA-8-3: Additional measures are necessary. The detailed risk assessment resulted in these additional measures. _ is implemented by: SP-SEC-DRA-8-1: The result of the initial risk assessment was VERY HIGH, see [SP-SEC-InitRiskAna]. _ is implemented by: SP-SEC-DRA-8-2: The acceptable and tolerable risk is MEDIUM.
IEC 63452 ZR-05-01	Perform Detailed Risk Assessment	The appointed organization, according to the Cybersecurity Management Plan, shall perform a detailed risk assessment on each zone and conduit of the SUC, which are impacted by initial risk exceeding the tolerable risk, where the initial risk exceeds the tolerable risk. The detailed risk assessment shall implement requirements from ZR-05-02 to ZR-05-11.	_ is implemented by: SP-SEC-DRA-2.1-1: The scope of the detailed risk assesement is based on the generic security architecture. This architecture can be mapped to detailed architectures used in projects.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-05-02	Identify threats	A list of the threats which could affect the assets contained in each zone or conduit shall be established and maintained.	_ is implemented by: SP-SEC-DRA-6-1: The threat envrionment is documented in the Threat Catalog [SP-SEC-ThreatCat].
IEC 63452 ZR-05-03	Identify Vulnerabilities	Analysis shall be performed on each zone or conduit to identify and document vulnerabilities associated with the assets contained within them, including their associated access points.	_ is implemented by: SP-SEC-DRA-11-1: [EU CRA] mandates to supply only devices without exploitable vulnerabilities. _ is implemented by: SP-SEC-DRA-11-2: Further discovered vulnerabilities are handled by vulnerability management process defined in [IEC 62443-4-1] and Chapter 13.3 of [SP-Sec-PrgmReq].
IEC 63452 ZR-05-04	Manage identified threats and vulnerabilities	All threats and vulnerabilities identified shall be addressed, either by: – using a code of practice (see 7.7.8), or – using a reference system (see 7.7.9), or – performing an explicit risk evaluation (see 7.7.10).	_ is implemented by: SP-SEC-DRA-9-2: The result of the detailed risk assessment is that the cybersecurity risk from the threat catalog is reduced to the risk level MEDIUM when applying the countermeasures of chapter 13.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-05-05	Apply a Code of Practice	In the application of a code of practice to mitigate a set of threats, the following points shall be fulfilled and documented: a) The code of practice is widely recognised, technically valid, lists the threats it addresses and provides justification for mitigation, and b) The code of practice is relevant to the SUC's selected threats, and c) The application of the code of practice is justified and documented in the Risk Assessment Report. Any deviations shall be justified and remaining risks shall be covered by either the use of a reference system or by performing an explicit risk evaluation.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-05-06	Application requirements from a reference system	In the application of a reference system, the following points shall be fullfiled and documented: – the reference system cybersecurity countermeasures are acceptable according to the current cybersecurity state-of-the-art; and – the reference system functions and interfaces are similar to the SUC; and – the operating environment and environmental conditions are similar; and – the reference system has a cybersecurity requirement specification, if not, the security requirements shall be collected from the documentation of the reference system and checked for correctness and completeness; and – all threats under consideration are considered to be effectively treated by the reference system; and – the application of requirements from a reference system is justified and documented in the Risk Assessment Report. Any deviations shall be justified and remaining risks shall be covered by either the use of a code of practice or by performing an explicit risk evaluation.	_ is implemented by: SP-SEC-DRA-2.1-2: The detailed risk assessment is part of the reference system applied in the context [CEN-CENELEC TS 50701:2023] and [IEC 63452], together with the SP Cybersecurity Specification main documents and supporting documents.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-05-07	Explicit Risk Evaluation - Calculate unmitigated risk	The unmitigated cybersecurity risk for each threat shall be determined by combining the unmitigated impact and the unmitigated likelihood.	_ is implemented by: SP-SEC-DRA-8-1: The result of the initial risk assessment was VERY HIGH, see [SP-SEC-InitRiskAna].
IEC 63452 ZR-05-08	Explicit Risk Evaluation - Determine SL-T	An SL-T shall be established for each security zone and conduit of the SUC, considering the unmitigated cyber security risk for each threat.	
IEC 63452 ZR-05-09	Explicit Risk Evaluation - Identify countermeasures to reduce the risk to a tolerable level	Cybersecurity countermeasures such as technical, administrative or procedural shall be identified to address all threats and vulnerabilities where the risk exceeds the tolerable risk, unless a documented decision was made by the asset owner to accept, avoid, or transfer the risk.	_ is implemented by: SP-SEC-DRA-13-1: The security countermeasures are documented in the following documents: • [SP-SEC-CompSpec] • [SP-SEC-CommSpec] • [SP-SEC-ServSpec] • [SP-Sec-PrgmReq]

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-05-10	Threats coverage and risk acceptance	Coverage of all identified risks shall be checked considering that any risk is either mitigated, or accepted, or avoided, or transferred.	_ is implemented by: SP-SEC-DRA-12-1: All risks in the threat catalog have been mititgated.

DRAFT

IEC 63452 ZR-05-11	Document results of the Detailed Risk Assessment	The results of the detailed risk assessment shall be documented and made available to the appropriate stakeholders, in the Risk Assessment Report. The risk assessment report shall include: – rationale for selection and applicability of a code of practice (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered – rationale for selection and applicability of a reference system (if selected), as well as threat coverage achieved, with respect to the sub-set of the SUC considered. – explicit risk evaluation results and methodology (if performed) – any assumptions made – If assumptions cannot be fulfilled by the SUC itself, they shall be exported as SecRACs. Furthermore, the following elements shall be documented: – Operating environmental assumptions – Risk acceptance criteria – Threat environment – List of vulnerabilities – Unmitigated risks – List of countermeasures (including SecRACs) – Residual risk and their status (avoided, accepted or transferred)	_ is implemented by: SP-SEC-DRA-2.2-1: This detailed risk assessment result can be used when implementing the generic security architecture.

DRAFT

IEC 63452 ZR-06-01	Cybersecurity Requirements Specification	The appointed organization, according to the Cybersecurity Management Plan, shall document all cybersecurity requirements results from the risk assessment in the cybersecurity requirements specification. The CRS shall include or refer to the following: 1) The SUC description (see ZR-01-01 in 7.3.4) 2) Zone and conduit drawings (see ZR-03-01 in 7.5.4) 3) Zone and conduit characteristics (see ZR-03-01 in 7.5.4), with their associated requirements: a) Security requirements based on the Risk Assessment Report (see ZR-05-11 in 7.7.12) b) SL-T, if applicable (see ZR-05-08 in 7.7.10.3) c) Assumptions (see ZR-05-11 in 7.7.12) d) Security-related application conditions (SecRACs) (see ZR-05-11 in 7.7.12) 4) Operating environment assumptions (see ZR-05-11 in 7.7.12) 5) The threat environment (see ZR-01-02 in 7.3.5) 6) Tolerable Risk (see ZR-04-01 in 7.6.4) 7) Regulatory requirements ((from legal team, tender requirements or contract). Cybersecurity requirements and security-related application conditions (SecRACs) shall be communicated to all the stakeholders of the SUC, which includes engineering, RAM, the safety team and the Asset Owner.	_ is implemented by: SP-SEC-Comp-4.2.6: Threat Environment _ is implemented by: SP-SEC-Comp-4.2.5: Operating Environment Assumptions _ is implemented by: SP-SEC-Comp-4.1: General SuC Description _ is implemented by: SP-SEC-Comp-4.2.4: Zone and Conduits Characteristics _ is implemented by: SP-SEC-Comp-4.2.3: Zone and Conduits Drawing _ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Regulatory Compliance Tracing, v1.1 _ is implemented by: SP-SEC-DRA-13-1: The security countermeasures are documented in the following documents: • [SP-SEC-CompSpec] • [SP-SEC-CommSpec] • [SP-SEC-ServSpec] • [SP-Sec-PrgmReq]

DRAFT

		Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation that was instrumental in performing the cyber risk assessment shall be recorded and archived along with the cyber risk assessment.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 ZR-07-01	Asset owner's approval	If the risk assessment is not performed by the asset owner, the asset owner shall review and approve the risk assessment report and the CRS.	_ is implemented by: SP-SEC-Pgrm-5-2: The railway shall ensure that the railway management bodies approve the cybersecurity risk-management measures.
IEC 63452 AA-01-01	Cybersecurity Architecture	The organization in charge of the SUC integration (in conformity with Cybersecurity Management Plan) shall devise a cybersecurity architecture for the railway solution that implements the functions necessary to meet the requirements defined in the CRS.	_ is implemented by: : The generic security architecture can be mapped to a specific security architecture. The figure below shows the mapping to the System Pillar scope.
IEC 63452 AA-01-02	Cybersecurity shall not adversely impact essential functions	Potential impact of implementation of cybersecurity requirements on essential functions shall be assessed and documented by the SI and accepted by the asset owner.	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Support for essential functions, v1.1

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 AA-01-03	System Cybersecurity Parametrisation	The the organization in charge of the SUC integration (in conformity with Cybersecurity Management Plan) shall devise the rules for parametrisation, document, apply in collaboration with the AO and check the correct application in the railway solution.	_ is implemented by: SP-SEC-DocTempl-5-14: <description which changes can affect the security of the products> _ is implemented by: SP-SEC-DocTempl-7-2: <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 effects on security, how to set, change and delete the configuration value>
IEC 63452 AA-01-04	Inclusion of compensating countermeasures	If a subsystem or component of the SuC does not meet the apportioned security requirements, the organization in charge of the SUC integration (in conformity with Cybersecurity Management Plan) shall evaluate the risks and address the changes as described in ZR-05-09 and any additional countermeasures (including SecRAC) shall be documented in a new version of the CRS. Compensating countermeasures shall be demonstrated to meet the same security objective intended by the original requirements and be documented. If needed, the requirement apportionment to sub-system and component shall be updated accordingly.	_ is implemented by: SP-SEC-Comp-2.2-3: If a requirement of this specification cannot be implemented (yet), the component documentation shall provide a justification for each non-implemented requirement, with respect to organisational needs, operational constraints and regulatory requirements (e.g. interface is not needed for operation, alternative mitigation, justified by an impact / risk analysis). _ is implemented by: SP-SEC-Comp-2.2-4: If a requirement of this specification cannot be implemented (yet), the component documentation shall include a description how to handle this case which has to be agreed with the asset owner (e.g. definition of a security related application condition).

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 AA-01-05	Cybersecurity Guidelines for the Railway Solution	The the organization in charge of the SUC integration (in conformity with Cybersecurity Management Plan) shall develop guidelines for the deployment operation and maintenance of the cybersecurity architecture implemented in the railway solution.	_ is implemented by: SP-SEC-DocTempl-9-1: <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> _ is implemented by: SP-SEC-DocTempl-8-1: <description of actions and responsibilities for user, including administrators>
IEC 63452 AA-02-01	Cybersecurity requirements traceability	Cybersecurity requirements shall be clearly identified covering all external and internal needs, and shall be traceable through a defined process to ensure complete and accurate tracking.	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Regulatory Compliance Tracing, v1.1

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 AA-03-01	Allocation to zone and conduit	Each cybersecurity requirement in CRS shall be allocated to the relevant zone and conduit and detailed so that they are: – Suited to the railway context; – Specific to the SUC; and – Applicable to the SUC.	_ is implemented by: : The attribute "Component Type" defines for which component type the requirement is applicable. • Requirements with component type "Generic" is applicable to all components except network components. See definiton Secure Component. • Requirements with component type "HMI" is only applicable for components with a Human Machine Interface (e.g. a component with a screen and interaction capabilities as keyboard, mouse, touch,...). See definition HMI Component. • Requirements with component type "Wireless" is only applicable for components with a wireless communication interfaces (e.g. IEEE 802.11, GSM, 5G, FRMCS,...). See definition Wireless Component. • Requirements with component type "Network" are applicable only for network components (see definition Network Component.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 AA-03-02	Requirements apportionment to subsystems	The the organization in charge of the SUC integration (in conformity with Cybersecurity Management Plan) shall apportion cybersecurity requirements identified during risk assessment as requirements at sub-system and component level.	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.1
IEC 63452 CA-01-01	Plan cybersecurity evaluation activities	The appointed organization, according to the cybersecurity management plan, shall develop a cybersecurity evaluation plan for assessing the cybersecurity design, implementation and configuration of the railway solution through the provision and examination of objective evidence.	

DRAFT

<table>
<tr>
<td>IEC 63452 CA-01-02</td>
<td>Independence of security testers</td>
<td>The system integrator shall apply a process to ensure that individuals performing testing are independent from the developers who designed and implemented the railway solution according to Table 6.

Table 6 – Required level of independence of testers from developers

<table>
<tr><th>Test type</th><th>Level of independence</th></tr>
<tr><td>Security requirements testing</td><td>Independent department</td></tr>
<tr><td>Threat mitigation testing</td><td>Independent department</td></tr>
<tr><td>Abuse case testing</td><td>Independent person</td></tr>
<tr><td>Static code analysis</td><td>None</td></tr>
<tr><td>Attack surface analysis</td><td>Independent person</td></tr>
<tr><td>Known vulnerability scanning</td><td>Independent person</td></tr>
<tr><td>Software composition analysis</td><td>None</td></tr>
<tr><td>Penetration testing</td><td>Independent department or organization</td></tr>
</table>

The levels of independence are defined as follows:

• None – no independence required. Developer can perform the testing.
• Independent person – the person who performs the testing cannot be one of the developers of the product.
• Independent department – the person who performs the testing cannot report to the same first line manager as any developers of the product. Alternatively, they could be a member of a quality assurance (QA) department</td>
<td>_ is implemented by: IEC 62443-4-1 SVV-5: Perform testing with independent personnel from product development.

_ is implemented by: 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.</td>
</tr>
</table>

DRAFT

		• Independent organization – the person who performs the testing cannot be part of the same organization as any developers of the product. An organization can be a separate legal entity, a division of a company or a department of a company that reports to a different executive such as a vice president or similar level.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CA-01-03	Execution of cybersecurity evaluation activities	The appointed organization, according to the cybersecurity management plan, shall execute all the activities described in its cybersecurity evaluation plan and document the methods, processes and results.	
IEC 63452 CA-01-04	Verification of cybersecurity deliverables	The appointed organization, according to the cybersecurity management plan, shall ensure that all cybersecurity deliverables defined in the evaluation plan are reviewed for completeness and consistency. Any identified issue shall be logged, communicated and addressed.	
IEC 63452 CA-01-05	Cybersecurity validation of the railway solution	The appointed organization, according to the cybersecurity management plan, shall demonstrate through the provision of objective evidence that the railway solution, in its operational configuration and with application of the documented SecRACs, meets the cybersecurity requirements of the CRS and that the cybersecurity risk level is acceptable according to the agreed risk acceptance criteria.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CA-01-06	Railway solution cybersecurity case	The appointed organization, according to the cybersecurity management plan, shall prepare the railway solution cybersecurity case. The railway solution cybersecurity case shall include or refer to: 1) the CRS; and 2) evidence demonstrating that the cybersecurity objectives have been fulfilled and the solution is fit for operation, such as verification and validation reports; and 3) information for the secure operation of the railway solution including the SecRACs; and 4) information on how cybersecurity risks affecting safety-related functions have been evaluated and how protection against the adverse influence has been achieved. NOTE This requirement and the corresponding guidance only address the cybersecurity case of the r ailway solution provided by the system integrator. The asset owner may maintain a cybersecurity case for their railway system that can refer to several cybersecurity cases from different system integrators (see [OM -03-01]).	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 CA-02-01	Establish cybersecurity handover plan	The appointed organization, according to the cybersecurity management plan, shall document a cybersecurity handover plan that includes all cybersecurity-related deliverables as well as activities to be performed during handover.	
IEC 63452 CA-02-02	Approval of the cybersecurity handover plan	The asset owner shall approve the cybersecurity handover plan.	
IEC 63452 CA-02-03	Approval of the cybersecurity case	The asset owner shall approve the railway solution cybersecurity case.	
IEC 63452 CA-02-04	Perform cybersecurity handover	The system integrator and the asset owner shall execute the activities specified in the cybersecurity handover plan, document the results and formally agree on its completion.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-01-01	Cybersecurity maintenance plan	The asset owner shall identify cybersecurity maintenance activities that are to be applied throughout the railway application life-cycle in a cybersecurity maintenance plan. The cybersecurity maintenance plan shall include at minimum the following topics in the context of the railway application: – Continuous cybersecurity verification – Railway application cybersecurity case update – Risk assessment update – Vulnerability management – Patch management – Incident management – Security monitoring – Decommissioning management	_ is implemented by: SP-SEC-DocTempl-9-1: <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> _ is implemented by: SP-SEC-DocTempl-9-3: <description how to verify authenticity and integrity of updates and how to install updates, including if a restart of the product is required> _ is implemented by: SP-SEC-DocTempl-10-1: <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>

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-01-02	Cybersecurity rules and procedures	The asset owner shall accept, adapt or establish and maintain cybersecurity rules and procedures to be applied during railway operation and maintenance activities addressing cybersecurity. These rules and procedures shall be based at minimum on: – The provided security guidelines from system integrator and product suppliers, – The OT cyber programme(s) and maintenance plan, – The asset owner experience, – The applicable regulations. These rules and procedures shall ensure full coverage of SecRACs of the railway solutions part of the railway application. These rules and procedures shall include at least : – Consistent access rules for operation and maintenance activities – Protection of critical data for operation and maintenance activities	_ is implemented by: : Europe's Rail System Pillar Cybersecurity Domain - Secure Program Requirements, v1.1

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-01-03	Continuous cybersecurity verification	The asset owner shall ensure that the activities defined in the cybersecurity maintenance plan and the SecRACs defined in the railway application cybersecurity case and cybersecurity guidelines are completely and correctly implemented, according the periodicity and criteria defined in the cybersecurity maintenance plan.	
IEC 63452 OM-02-01	Railway application cybersecurity case	The asset owner shall establish and maintain a railway application cybersecurity case. The railway application cybersecurity case shall include or refer the railway solution cybersecurity case(s) and the evidence of the application of SecRACs and of applicable cybersecurity rules and procedures. The railway application cybersecurity case shall be established before railway application start of service. The railway application cybersecurity case shall be periodically checked and updated if necessary, according criteria defined in the cybersecurity maintenance plan.	

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-03-01	Risk assessment update	The asset owner shall review the risk assessment according to periodicity and criteria defined in the cybersecurity maintenance plan, update it if necessary, and treat cybersecurity risks.	
IEC 63452 OM-04-01	Vulnerability advisories	The asset owner shall have a process to request and integrate vulnerability advisories from stakeholders of the supply chain.	_ is implemented by: SP-SEC-Pgrm-8.1-2: The railway shall require the suppliers to follow a coordinated vulnerability disclosure procedure according to ISO 29147. _ is implemented by: 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.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-04-02	Vulnerability management	The asset owner shall establish, maintain and apply a vulnerability management process to identify, analyse and resolve vulnerabilities from internal and external sources. This process shall include: – organisational aspects (roles and responsibilities allocation), – communication aspect (including report and disclosure), – process scoping, – vulnerability identification, analysis and prioritization criteria, – vulnerability handling decision (accept the risk, mitigate, remediate).	_ is implemented by: SP-SEC-Pgrm-8.1-5: The railway shall define procedures for the vulnerability management process of the Secure Component based on ISO 27002 chapter 8.8.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-05-01	Patch management process	The asset owner shall establish, maintain and apply a patch management process for the railway application that includes: – identification of the component capabilities related to patching, – identification of all stakeholders with their roles and responsibilities, – monitoring of availability of patches with security fixes for each component, – patch prioritization, selection, testing, and deployment schedule, – patch deployment activities, – verification that patches have been correctly applied.	_ is implemented by: 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.
IEC 63452 OM-05-02	Patch management supply chain	The asset owner shall establish, document and maintain patch management requirements for product supplier, system integrator and maintenance service provider (see clause 5.8).	_ is implemented by: SP-SEC-Pgrm-8.1-2: The railway shall require the suppliers to follow a coordinated vulnerability disclosure procedure according to ISO 29147.
IEC 63452 OM-05-03	End-of-life and end-of-security-support considerations	The asset owner shall monitor the end-of-life and end-of-security-support (no more security updates provided) of railway application's asset and anticipate decisions to be able to operate its railway application in a secure state.	_ is implemented by: SP-SEC-DocTempl-3-4: <end-date (month and year) for vulnerability handling and security update support. The end-date should be the expected use-time, at least five years unless the expected use-time is less than five years>

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-06-01	Incident management	The asset owner shall establish, maintain and apply a process for evaluating and responding to cybersecurity incidents affecting the railway application. The incident management process shall address the following aspects: – communication channels, roles and responsibilities for receiving incident notifications and reacting in a timely manner, – assessing the impact of the incident and defining and applying the countermeasures needed to contain, resolve and recover from the incident, – reporting to authorities or other entities (like ISACs) about ongoing or past incidents, – identifying lessons learnt to eliminate the causes or reduce the likelihood for similar incidents in the long term, – documenting accepted risks associated with incidents.	_ is implemented by: SP-SEC-Pgrm-11-13: The railway shall define an incident handling and response process based on ISO 27002 chapter 5.26.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-07-01	Security monitoring	The asset owner shall establish security monitoring capabilities in order to ensure detection, reporting, handling, and timely response to security events in its railway application. The asset owner shall define the scope of security monitoring (the concerned railway applications or a part of them) according to risk management conclusions and regulatory constraints.	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-11-1: The railway shall define a logging strategy, integrating legacy and new systems. _ is implemented by: SP-SEC-Pgrm-11-1: The railway shall define logging requirements based on ISO 27002 chapter 8.15.

DRAFT

IEC 63452	Topic	Requirement	implemented by
IEC 63452 OM-08-01	Decommissioning management	The asset owner shall establish, maintain and apply a documented process for decommissioning or removal of subsystems and components, referring cybersecurity guidelines when available, to ensure that no cybersecurity-related sensitive information can be extracted.	_ is implemented by: 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. _ is implemented by: SP-SEC-Pgrm-9.2-7: The railway shall change the status of the Secure Component in the asset management system to "decommissioned" after successful decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.2-4: The railway shall revoke certificates of the Secure Component during decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.2-5: The railway shall remove all access rights of the Secure Component during decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.2-1: The railway shall document the decommissioning process. _ is implemented by: SP-SEC-Pgrm-9.2-3: The railway shall require and establish procedures to securely destroy equipment if purging data is not possible.
68 items found			

DRAFT