Disclaimer

This document is

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

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

drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

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

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

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

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

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address:

cybersecurity.review@ertms.be

1 Table of Contents

Work Item Type	Icon	Rationale
System Requirement	📝	Used for mandatory requirements.
Text	📄	Used for prose text, e.g. as an introduction or for additional information. The contents of these work items are **not requirements.**
Issue	☰	Used for open issues to be addressed in the final version. The contents of these work items are **not requirements.**
Reference	⧉	Used for references to external documents. The contents of these work items are **not requirements.**
Definition	📋	Used for term definitions. The contents of these work items are **not requirements.**

First draft version (01/2024) includes:

- Import of EULYNX BL 4 R2 and ESCG content
- review of requirements
- alignment to taxonomy and TSI CCS 2023
- deletion of duplicates
- improvement of requirement language (testability, tracing to norms)
- internal review by System Pillar Cybersecurity domain
- mapping table to IEC 62443-4-2, CRA, CLC/TS 50701
- in progress CSA, RED, IEC 63452

Second draft version (02/2024) includes

- updated according to review comments from 1st draft review

Final draft (03/2024) includes

- updated according to review comments from 2nd draft review
- new specification text to close the open issues

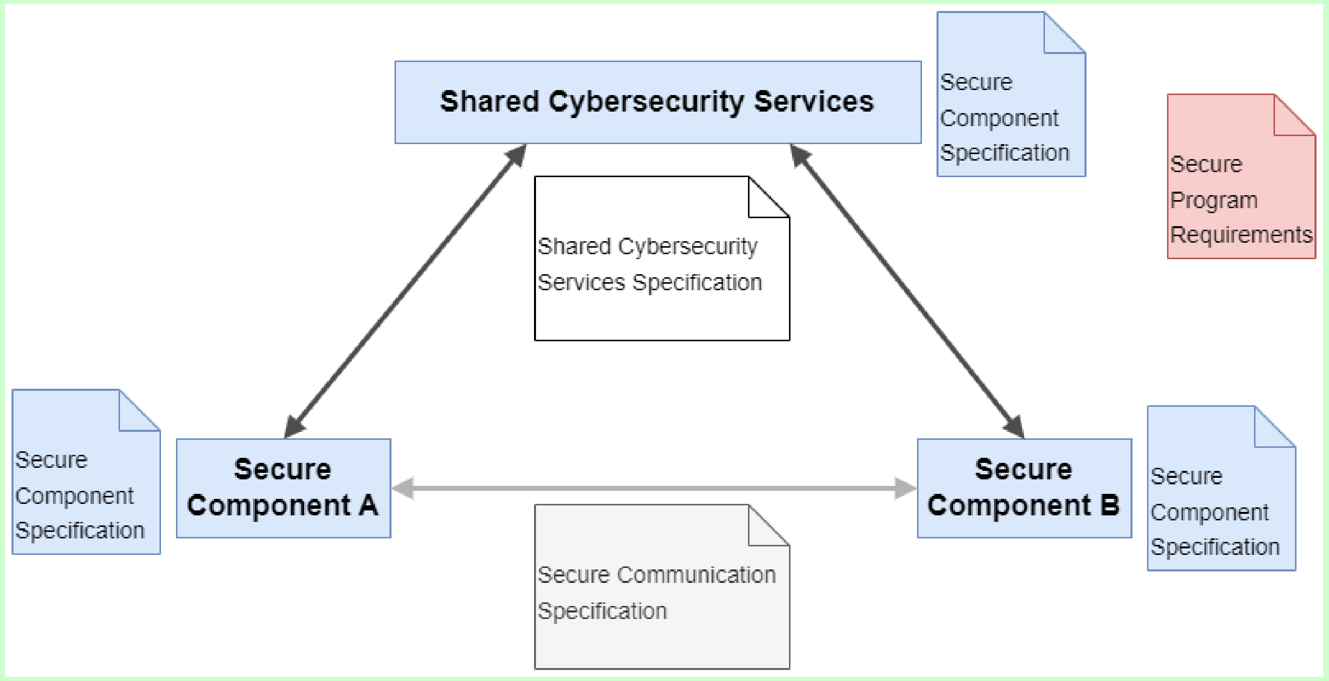
, SP-SEC-Comp-32.1-1 - This specification is a Cybersecurity Requirements Specification (CRS) according with [IEC 62443 and TS 50701 (IEC 63452). **[** Open, SPPRAMSS-9659 -3-2:2020], [CEN-CENELEC TS 50701:2023] and [IEC PT 63452]

, SP-SEC-Comp-32.1-2 - This CRS is intended to be used as a protection profile and could be used together with the evaluation method defined in a canditate for a certification scheme compatible to the EU CSA together with an evaluation method (as being defined in upcoming IEC 62443-6-2 under a certification scheme compatible to the EU CSA. **[** Open, SPPRAMSS-9646 **]**).

, SP-SEC-Comp-32.1-3 - The following figure shows the relationship of this specification to the key terms and other referenced specifications. **[** Open, SPPRAMSS-9647 **]**

, SP-SEC-Comp-32.1-4 - Key terms and technical specs used in the System Pillar Cyber Security domain

[Open, SPPRAMSS-7034 **]**this document.


Shared Cybersecurity Services
Secure Component Specification
Secure Program Requirements
Shared Cybersecurity Services Specification
Secure Component Specification
Secure Component A
Secure Component B
Secure Component Specification
Secure Communication Specification

, SP-SEC-Comp-32.1-5 - In particular this CRS does not define:

· Detailed requirements for Secure Communication. These requirements can be found in 21 the Secure Communication Specification[SP-SEC-CommSpec] .

· Requirements for the interfaces to the shared cybersecurity services. These requirements can be found in . 22 the Shared Cybersecurity Services Specification[SP-SEC-ServSpec]

· Security life-cycle requirements, including operational requirements. These requirements can be found in 60_Security_Program_Requirements old.

[Open, SPPRAMSS-9626 **]**
Shared Cybersecurity Services Interface Specification [SP-SEC-PrgmReq].

, SP-SEC-Comp-32.1-6 - The Secure Component specification shall be applied has been specified to be used together with the Shared Cybersecurity Services Specification and the Secure Communication Specification. **[**SPPRAMSS-9628, Generic , no **]**

, SP-SEC-Comp-32.1-7 - Secure Components (see definition Secure Component) connect to a communication network. The security functionality defined in this specification requires certain functions of network components. These requirements related to network devices are marked in this spec specification with the component type "Network Component" . **[** Open, SPPRAMSS-9630 **]**(see definiton Network Component).

, SP-SEC-Comp-32.1-8 - 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 User 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 SPPRAMSS-4723 - definition Network Component

[Open, SPPRAMSS-9621 **]**

- .

, **SP-SEC-Comp-2.2-1 -** This specification includes all requirements required for protection against threats defined in the generic risk assessment (see SP-SEC-CompSpec Ch 4.2.7 - Threat and risk analysis result) and compliance to various standards (see [Document base]).

, **SP-SEC-Comp-2.2-2 -** The requirements in this specification are intended to lead to harmonised security of Secure Components in the market (level playing field). Deviations, if any, should be kept to a minimum and are only possible when documented by the following two requirements.

, **SP-SEC-Comp-2.2-3 -** If a requirement of this specification can't be implemented (yet), the component documentation shall include documentation of non-implemented requirements and justification for each non-implemented requirement (e.g. interface is not needed for operation, alternative mitigation, justified by impact / risk analysis). **[**Generic **]**

, **SP-SEC-Comp-2.2-4 -** If a requirement of this specification can't 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). **[**Generic **]**

, **SP-SEC-Comp-2.2-5 -** This specification uses identifiers starting with "SP-SEC-Comp".

, **SP-SEC-Comp-2.2-6 -** References, taxonomy, key terms, and icon types used in this document are defined in [SP-SEC-Tax].

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

- [SP-SEC-Tax]
Europe's Rail System Pillar Cybersecurity Domain - Taxonomy and References, v1.0

, **SP-SEC-Comp-3.2-1 -** **- [Document base]**

This CRS was developed based on:

- [IEC 62443-4-2 Ed 1EULYNX BL4 R2:2019]
- [EULYNX/EU-Rail BL4 R3]
- ESCG Requirements
- [UNISIG Subset SUBSET-146 v4.00]
- [UNISIG Subset SUBSET-147 v4.00]
- [CEN-CENELEC TS 50701/:2023] and

- [IEC PT 63452

[Open, SPPRAMSS-9623]

-] (draft version Jan 2025)

- [SP-SEC-ThreatAna]

Europe's Rail SystemPillar Cybersecurity Domain - Intial Threat Analysis, v1.0

- [SP-SEC-

Comp-3.2-2 - IEC 62443-4-1 Ed 1

IEC 62443-4-1 Ed 1 Secure product development lifecycle requirements **[**SPPRAMSS-9624 **]**

, SP-SEC-Comp-3.2-3 - MinElements_SBOM

ThreatCat]

Europe's Rail SystemPillar Cybersecurity Domain - Threat Catalog, v1.0

- [SP-SEC-DocTempl]

Europe's Rail SystemPillar Cybersecurity Domain - Product Documentation Template, v1.0

- [SP-SEC-CompSpec]

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

- [SP-SEC-CommSpec]

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

- [SP-SEC-ServSpec]

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

- [SP-SEC-PrgmReq]

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

- [RFC 4086]

Randomness Requirements for Security

- [IEC 62443-4-1:2018]

Secure product development lifecycle requirements

- [MinElements_SBOM]

The Minimum Elements for an SBOM

https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf **[**SPPRAMSS-9618 **]**

- [CIS benchmark]

Operating System and application specific benchmarks, regularly updated

List of available benchmarks, use latest and the most specific benchmark matching the operating system and/or application.

- [UNISIG SUBSET-146 v4.00]

ERTMS End-to-End security layer (TLS layer for ETCS and ATO communication), v4.0

- [UNISIG SUBSET-147 v4.00]

CCS Consist network communication layer, V4.0

- [UNISIG SUBSET-137 v4.00]

ETCS On-line Key Management, v4.0

- [CEN-CENELEC TS 50701:2023]

Railway applications - Cybersecurity

- [IEC PT 63452]

Railway applications - Cybersecurity - January 2025 draft

- [IEC 62443-3-2:2020]

Security risk assessment for system design

- [ISO/IEC 27001:2022]

Information security, cybersecurity and privacy protection - Information security management systems - Requirements

- [IEC 62443-2-1:2024]

Security program requirements for IACS asset owners

- [IEC 62443-2-4:2023]

Security program requirements for IACS service providers

- [IEEE 802.1Q-2018]

IEEE Standard for Local and Metropolitan Area Networks-Bridges and Bridged Networks

ATO - Automatic Train Operation

CCS - Control Command and Signalling

CMP - Certificate Management Protocol

COTS - Commercial-off-the-shelf

CPU - Central Processing Unit

CRA - Cyber Resilience Act

CRL - Certificate Revocation List

CRS - Cybersecurity Requirement Specification

DNS - Domain Name System

DMZ - Demilitarized Zone

DoS - Denial of Service

EU - European Union

ETCS - European Train Control Sysem

FQDN - Fully Qualified Domain Name

GDPR - General Data Protection Regulation

HMI - Human Machine Interface

IAM - Identity and Access Management

IACS - Industrial Automation Control System

I/O - Input / Output

IT - Information Technology

IXL - Interlocking

LAN - Local Area Network

OB - Onboard

OT - Operational Technology

PKI - Public Key Infrastructure

RBC - Radio Block Centre

SBOM - Software Bill of Material

SC - Secure Component

SCS - Shared Cybersecurity Services

SNMP - Simple Network Management Protocol

SUC - System under Consideration

SSI - Standard Security Interfaces

TS - Trackside

VLAN - Virtual LAN

WLAN - Wireless LAN

, SP-SEC-Comp-32.45-1 - Secure Component

An implementation, as part of the rail an automation control system, which comprises system components, such as host deviceseither a host device, embedded devicesdevice, network devices device or software applications, that implement application on a host device, which realizes subsystem functions, implements security capabilities and consisting of a physical encasing, computing capabilities and network communication, and interfacing to the Shared Cybersecurity Services.

Examples of CCS secure components are object controller, trackside cabinet, IXL rack, ATO-OB, OBU, ATO-TS, IXL/RBC combination, shared cybersecurity services…) [SPPRAMSS-1447]

services, security proxy for legacy devices, …)

Examples of components which are not meeting the definition of a Secure Component are components with no network communication, e.g. directly connected sensors or displays.

, SP-SEC-Comp-32.45-2 - Shared Cybersecurity Services (SCS)

A collection of standard security interfaces (SSIs) of central security functions accessible for all Secure Components in the automation solution. The realization of the Shared Cybersecurity Services (SCS) implement implements the requirements of the Secure Component Specification as they are considered also are as Secure Components as well.

The interfaces from Secure Components to Shared Cybersecurity Service are identified by SCSby SSI-<service name>.

Standard Security Interfaces

The Shared Cybersecurity Services implementations are identified by SSIby SCS-<service name>. [SPPRAMSS-1446]<service name>.

, SP-SEC-Comp-32.45-3 - Enterprise Cybersecurity Services (ECS)

A collection of enterprise security interface (ESI) implementations of central security and IT communication functions in a back-office environment.

Examples are Security Incident and Event Management System (SIEM), Intrusion Detection System, PKI Certificate Authority, Corporate Directory, Asset Management, DNS. These services are typically accessible for the automation network via controlled communication paths (e.g. DMZ). The interfaces of the Shared Cybersecurity Services to the Enterprise Services are identified by ESI-<Service name>.

Note: Enterprise Shared Services are typically 3rd-party components not dedicated to the rail environment. Therefore the realization of the Enterprise Shared Services may use other security requirements than the Secure Component Specification. Recommended security specification are ISO 27033, ISO 27034, NIST 800-53, and/or IEC 62443-4-2,…

[SPPRAMSS-6720]

.

Note: Enterprise Shared Services and Shared Cybersecurity Services are separated by the IT/OT border (e.g. by a DMZ).

, SP-SEC-Comp-32.45-4 - Network Component

An implementation of data networking functions such as switching, routing, filtering or tunneling.A device that facilitates IP data flow between devices, or restricts the flow of data, but may not directly interact with a control process.

Examples of Network Components are network switches, LAN/WAN routers, firewalls, data diodes and VPN endpoints.

Excluded are from this definition are media converters, transceivers and bridges with no routing, switching or filtering capabilities. [SPPRAMSS-4723]Such devices are not affected by this specification.

, SP-SEC-Comp-32.45-5 - Wireless Component

A Secure Component or Network Component with a wireless communication interface.
Examples of Wireless Components are handheld devices, WLAN access points, WLAN/5G/FRMCS/... routers, modems and wireless object controllers,....

Note: additional requirements apply to Wireless Components (as SR IEC 62443-4-2 NDR 1.6, SR NDR 1.6 RE1 and SR CR 2.2, SR CR 2.2 RE1) [SPPRAMSS-4721]

, SP-SEC-Comp-32.45-6 - HMI Component

A Secure Component with a human user machine interface.
Examples of HMI Components are PC Workstation, tablet device, smart phone, device with touch screen,...

Exemptions: embedded components without a screen, e.g. with push buttons and LEDs. [SPPRAMSS-4722]

, SP-SEC-Comp-

3

2.

4

5-7 - Essential Function

Function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under

control

control (definition from IEC 62443-4-2)

Note

1 to the entry

: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

In the context of the ERJU System Pillar all systems in scope provide functionality as defined in "Essential functions".

Note: IEC 63452 definition: All functions needed to operate the railway system, such as per example traffic control, speed control, traction/brake control,...

[SPPRAMSS-9640]

, SP-SEC-Comp-

3

2.

4

5-8 - Threat landscape

Threat landscape is used in this document as synonym for threat environment.

Threat environment (definition from CENELEC TS 50701, IEC PT 63452)

environment summary of information about threats, such as threat sources, threat vectors and trends, that have the potential to adversely impact a defined target (for example a company, facility or SuC)

[SPPRAMSS-9642 **]**

, SP-SEC-Comp-3.5-1 - This specification includes all requirements required for protection against risks defined in the generic risk assessment (see 4.2.7 - Threat and risk analysis result) and compliance to various standards (see SPPRAMSS-1456 - Regulatory requirements mapping). **[** Open, SPPRAMSS-9636 **]**

, SP-SEC-Comp-3.5-2 - The requirements in this specification are intended to lead to harmonised security of components in the market (level playing field). Deviations, if any, should be kept to a minimum and are only possible when documented by the following two requirements. **[** Open, SPPRAMSS-10321 **]**

, SP-SEC-Comp-3.5-3 - If a requirement of this specification is not implemented, the component documentation shall include documentation of non-implemented requirements and justification for each non-implemented requirement (e.g. interface is not needed for operation, alternative mitigation, justified by impact / risk analysis). **[**SPPRAMSS-9637, Generic , no **]**

, SP-SEC-Comp-3.5-4 - If a requirement of this specification is not implemented, the component documentation shall include a description how to handle this case which has to be agreed with the system integrator (e.g. definition of a security related application condition). **[**SPPRAMSS-9638, Generic , no **]**

First release (V1.0) - February 2025

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

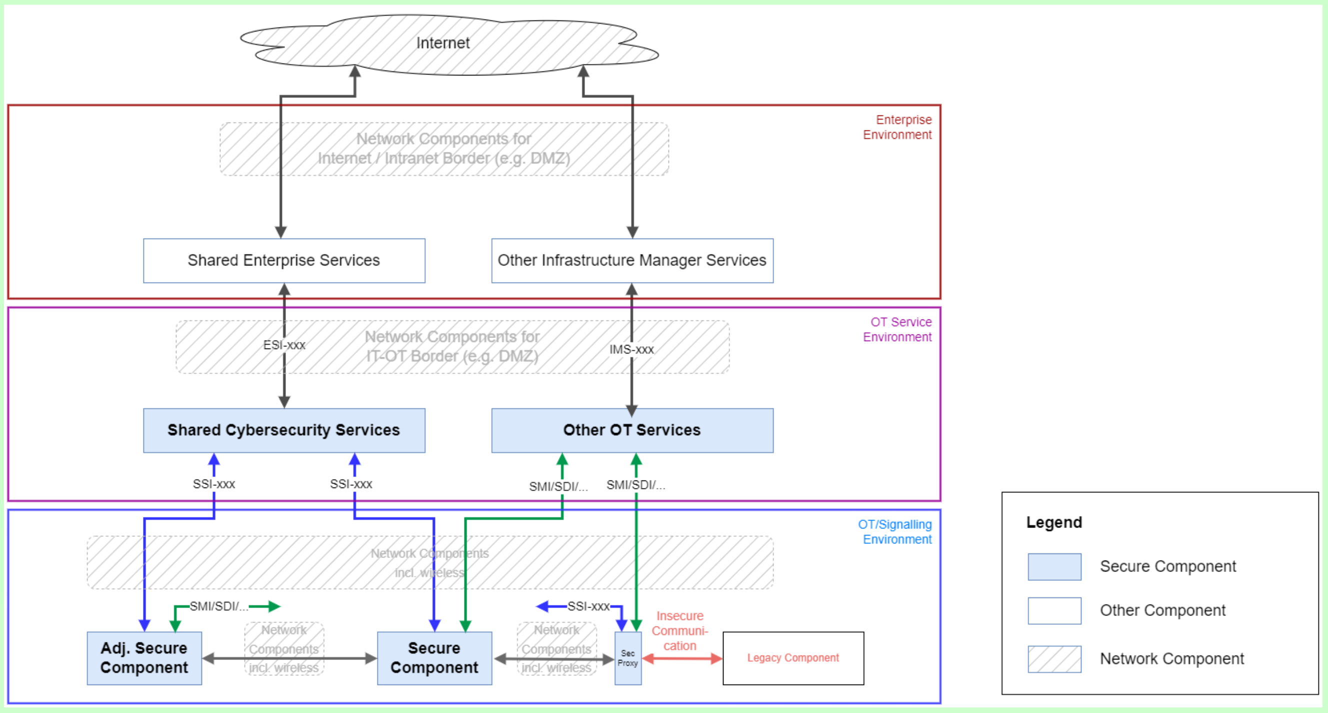
Intentionally left blank.

This chapter contains the required information for a cybersecurity requirements specification (CRS) as defined in IEC 62443-3-2 ZCR-6-1, CENELEC TS 50701 chapter 7.2.10 and IEC 63452 ZR-0406-1101.

, SP-SEC-Comp-4.1-1 - The System under Consideration (SuC) in the context of this specification is the Secure Component. **[** Open, SPPRAMSS-9657 **]**

, SP-SEC-Comp-4.1-2 - The Secure Component is highlighted in orange Components are shown in blue color in the figure below for main purpose of SuC description. The items in blue are also Secure Components:

[Open, SPPRAMSS-10370 **]**


Internet
Enterprise Environment
Network Components for Internet / Intranet Border (e.g. DMZ)
Shared Enterprise Services
Other Infrastructure Manager Services
OT Service Environment
ESI-xxx
Network Components for IT-OT Border (e.g. DMZ)
IMS-xxx
Shared Cybersecurity Services
Other OT Services
SSI-xxx
SSI-xxx
SMI/SDI/...
SMI/SDI/...
OT/Signalling Environment
Network Components incl. wireless
SMI/SDI/...
SSI-xxx
Network Components incl. wireless
Network Components incl. wireless
Insecure Communi-cation
Adj. Secure Component
Secure Component
Sec Proxy
Legacy Component
Legend
Secure Component
Other Component
Network Component

, SP-SEC-Comp-4.1.1-1 - The Secure Component, as per definition SPPRAMSSSP-1447 - SEC-CompSpec Ch 3.5 - Secure Component , has a physical encasing which defines the SuC boundary, and has computing and network communication capabilities. **[** Open, SPPRAMSS-10373 **]**

, SP-SEC-Comp-4.1.1-2 - The standard scope for Secure Components is the automation environment, also called operational technology environment (OT), which contains mainly embedded devices, some devices with an HMI, and network communication devices. In the figure above, the OT/signalling environment and OT service environment contain Secure Components. **[** Open, SPPRAMSS-10379 **]**

, SP-SEC-Comp-4.1.1-3 - Outside of the scope for Secure Components are enterprise Enterprise environments, also called back-office environments. Also , and cloud environments are outside the scope for of Secure Components. These environments have adhere to different security standards and security specifications. However, if applications or services in within the back office or cloud environment are part of the rail domain, the use of the Shared Cybersecurity Services interfaces could and parts of this specification may be applicable. The use of these interfaces will be described in the corresponding TSIs. **[** Open, SPPRAMSS-10377 **]**

, SP-SEC-Comp-4.1.1-4 - Outside of the scope for Secure Components are train components which Train components that do not reside in the signaling environment . A modern train integrates are outside the scope of Secure Components specification. Modern trains integrate hundreds of components from a large number of numerous suppliers which differs vary from country to country. Therefore, special care should be used when applying this or parts of the specification (e.g. for CRA compliance) to other parts of the train than the signaling environment. **[** Open, SPPRAMSS-10378 **]**

, SP-SEC-Comp-4.1.1-5 - For the rail automation / CCS scope, examples of secure components are object controller, trackside cabinet, IXL rack, ATO-OB, OBU, ATO-TS, IXL/RBC combination, shared cybersecurity services… **[** Open, SPPRAMSS-10371 **]**

, 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. **[** Open, SPPRAMSS-10382 **]**

, SP-SEC-Comp-4.1.2-2 - Essential functions of a Secure Components Component are all control functions which maintain health, safety, the environment and availability for the equipment the equipment under control (see definition SPPRAMSSSP-9640 - SEC-Comp-3.5-7 - Essential Function Definition). Typical examples are include safety-related functions which includes that allow the ability operator to control and for the operator to , view, and manipulate the system under control. **[** Open, SPPRAMSS-10380 **]**supervision.

, SP-SEC-Comp-4.1.3-1 - A Secure Component can have has the following interfaces:

1. Interfaces to a adjacent Secure Components via TLS, typically involving safety-related communication, specified in SecCommSpec Ch. 4 End-to-End Security Layervia protocols defined in SecCommSpec
2. Interfaces to Shared Cybersecurity Services, specified in [SP-SEC-SERV ServSpec] - Shared Cybersecurity Services specification interface specification
3. Interfaces to OT Shared Services defined by SMI and SDI, specified in System Pillar & EULYNX publication of BL4 R2 (EU.Doc 76 and EU.Doc. 77) and SecCommSpec SP-SEC-CommSpec Ch. 5 4 - Secure Communication for OPC UA
4. Interfaces to other components/services, specified in Chapter 7.5 Components with additional communicating processes

[Open, SPPRAMSS-10381 **]**

1. All other interfaces, for which SP-SEC-CommSpec Ch 6- Securing other communicating interfaces is applicable

, SP-SEC-Comp-4.1.4-1 - Secure Components interact with other Secure Components to support the essential functions. Examples for assets supporting an essential functions are:

- an interlocking interacts with object controllers to set a route for a train
- an RBC sending a movement authority to a train involving the Onboard unit (OBU) / European Vital Computer (EVC).

[Open, SPPRAMSS-10384 **]**

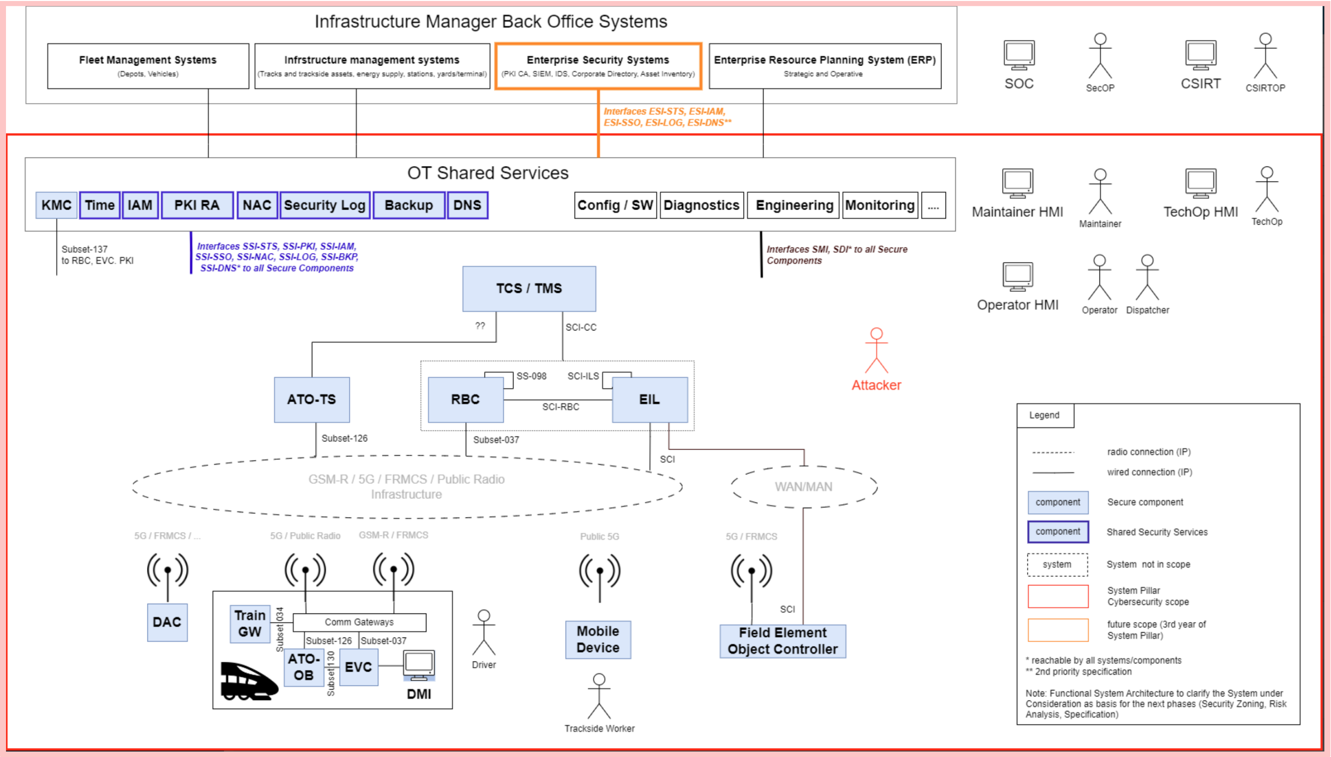
, SP-SEC-Comp-4.2.1-1 - The generic security architecture is defined in SP-SEC-Comp -Ch 4.1 - 2 **[** Open, SPPRAMSS-9656 **]**General SuC Description

, SP-SEC-Comp-4.2.2-1 - The generic security architecture can be mapped to a specific security architecture. The figure below show shows the mapping to the system pillar System Pillar scope. **[** Open, SPPRAMSS-10385 **]**

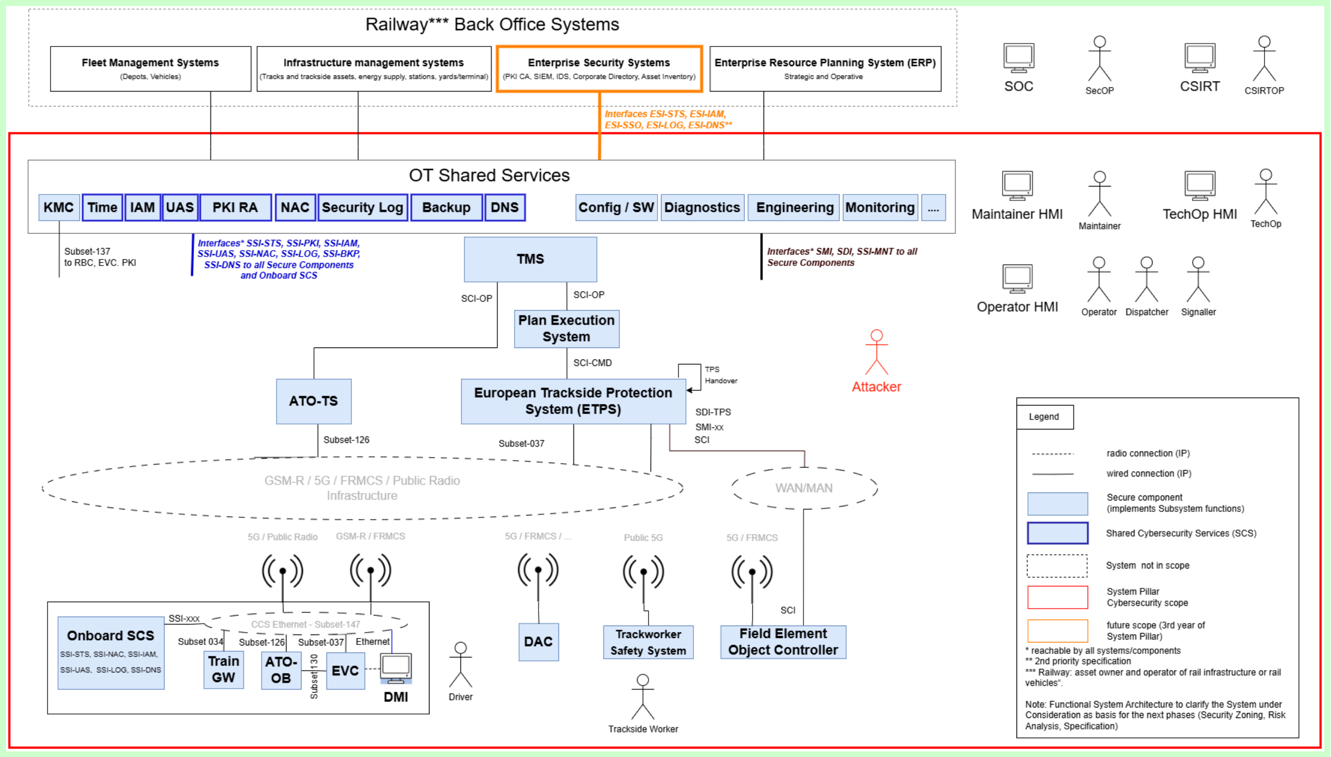
, SP-SEC-Comp-4.2.2-2 -

Cyber Security

Cybersecurity Architecture for an example rail automation system following the ERJU System Pillar Future Architecture approach based on definitions in [CLS:TS 50701:2023] and [IEC 62443-3-3:2013] .

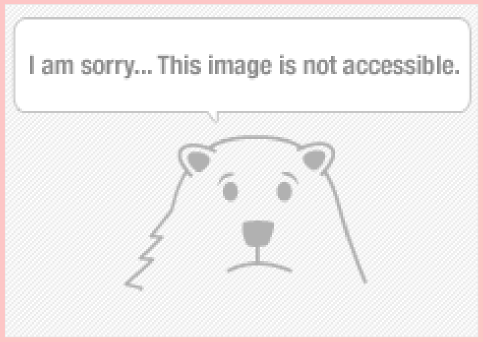

Infrastructure Manager Back Office Systems
Fleet Management Systems
(Depots, Vehicles)
Infrstructure management systems
(Tracks and trackside assets, energy supply, stations, yards/terminal)
Enterprise Security Systems
(PKI CA, SIEM, IDS, Corporate Directory, Asset Inventory)
Enterprise Resource Planning System (ERP)
Strategic and Operative
Interfaces ESI-STS, ESI-IAM, ESI-SSO, ESI-LOG, ESI-DNS**
SOC
SecOP
CSIRT
CSIRTOP
OT Shared Services
KMC
Time
IAM
PKI RA
NAC
Security Log
Backup
DNS
Config / SW
Diagnostics
Engineering
Monitoring
....
Maintainer HMI
Maintainer
TechOp HMI
TechOp
Subset-137 to RBC, EVC. PKI
Interfaces SSI-STS, SSI-PKI, SSI-IAM, SSI-SSO, SSI-NAC, SSI-LOG, SSI-BKP, SSI-DNS* to all Secure Components
Interfaces SMI, SDI* to all Secure Components
Operator HMI
Operator
Dispatcher
TCS / TMS
??
SCI-CC
SS-098
SCI-ILS
ATO-TS
RBC
SCI-RBC
EIL
Attacker
Subset-126
Subset-037
SCI
GSM-R / 5G / FRMCS / Public Radio Infrastructure
WAN/MAN
5G / FRMCS / ...
5G / Public Radio
GSM-R / FRMCS
Public 5G
5G / FRMCS
DAC
Train GW
Subset 034
Comm Gateways
Subset-126
Subset-037
ATO-OB
Subset 130
EVC
DMI
Driver
Mobile Device
Trackside Worker
SCI
Field Element Object Controller
Legend
radio connection (IP)
wired connection (IP)
component
Secure component
component
Shared Security Services
system
System not in scope
System Pillar Cybersecurity scope
future scope (3rd year of System Pillar)
* reachable by all systems/components
** 2nd priority specification
Note: Functional System Architecture to clarify the System under Consideration as basis for the next phases (Security Zoning, Risk Analysis, Specification)

[Open, SPPRAMSS-10387]

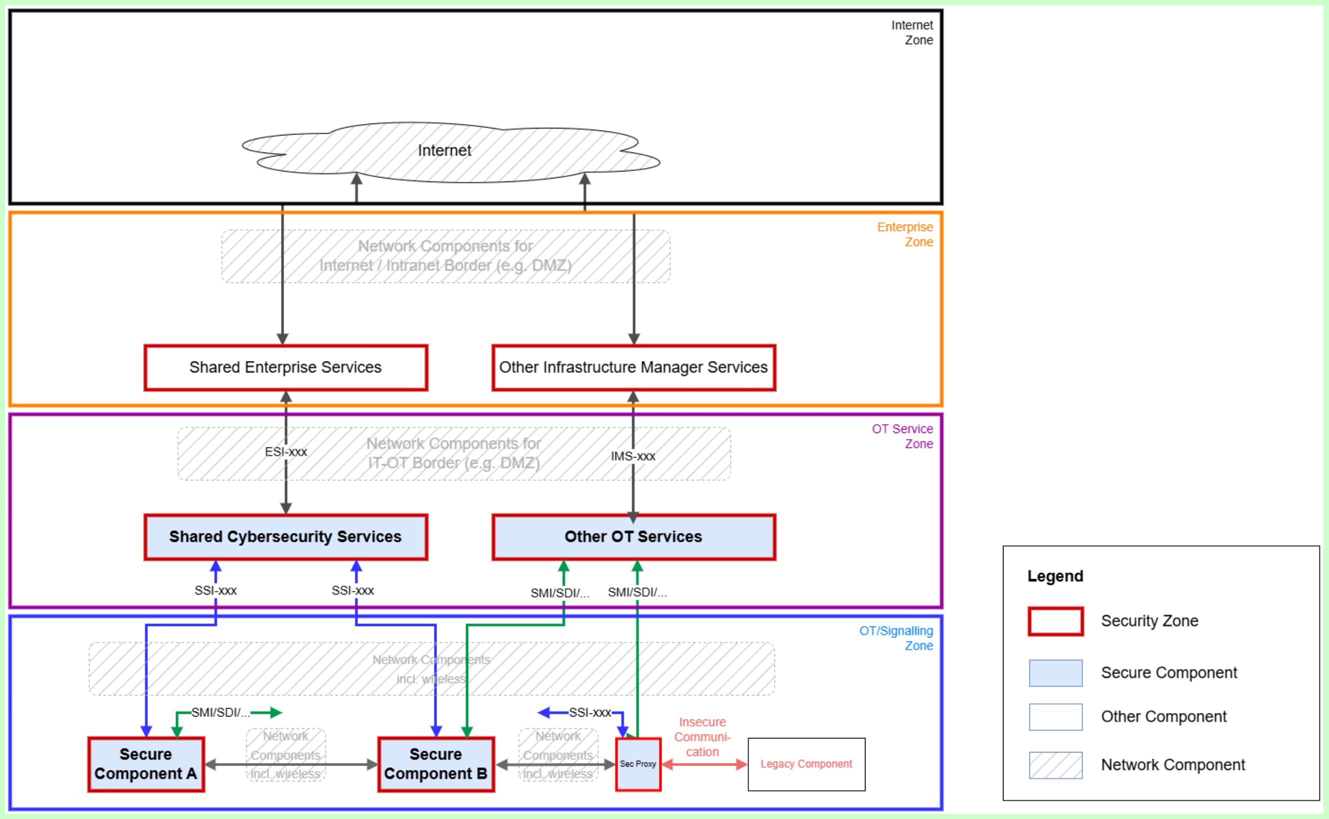

Railway*** Back Office Systems
Fleet Management Systems
(Depots, Vehicles)
Infrastructure management systems
(Tracks and trackside assets, energy supply, stations, yards/terminal)
Enterprise Security Systems
(PKI CA, SIEM, IDS, Corporate Directory, Asset Inventory)
Enterprise Resource Planning System (ERP)
Strategic and Operative
Interfaces ESI-STS, ESI-IAM, ESI-SSO, ESI-LOG, ESI-DNS**
SOC
SecOP
CSIRT
CSIRTOP
OT Shared Services
KMC
Time
IAM
UAS
PKI RA
NAC
Security Log
Backup
DNS
Config / SW
Diagnostics
Engineering
Monitoring
....
Maintainer HMI
Maintainer
TechOp HMI
TechOp
Subset-137 to RBC, EVC. PKI
Interfaces* SSI-STS, SSI-PKI, SSI-IAM, SSI-UAS, SSI-NAC, SSI-LOG, SSI-BKP, SSI-DNS to all Secure Components and Onboard SCS
TMS
Interfaces* SMI, SDI, SSI-MNT to all Secure Components
Operator HMI
Operator
Dispatcher
Signaller
SCI-OP
SCI-OP
Plan Execution System
SCI-CMD
TPS Handover
Attacker
ATO-TS
European Trackside Protection System (ETPS)
SDI-TPS
SMI-xx
SCI
Subset-126
Subset-037
GSM-R / 5G / FRMCS / Public Radio Infrastructure
WAN/MAN
5G / Public Radio
GSM-R / FRMCS
5G / FRMCS / ...
Public 5G
5G / FRMCS
SSI-xxx
CCS Ethernet - Subset-147
Onboard SCS
SSI-STS, SSI-NAC, SSI-IAM, SSI-UAS, SSI-LOG, SSI-DNS
Subset 034
Subset-126
Subset-037
Ethernet
Train GW
ATO-OB
Subset 130
EVC
DMI
Driver
DAC
Trackworker Safety System
Trackside Worker
SCI
Field Element Object Controller
Legend
radio connection (IP)
wired connection (IP)
Secure component (implements Subsystem functions)
Shared Cybersecurity Services (SCS)
System not in scope
System Pillar Cybersecurity scope
future scope (3rd year of System Pillar)
* reachable by all systems/components
** 2nd priority specification
*** Railway: asset owner and operator of rail infrastructure or rail vehicles".
Note: Functional System Architecture to clarify the System under Consideration as basis for the next phases (Security Zoning, Risk Analysis, Specification)

Note: the red rectangular defines the scope of the ERJU System Pillar. The architecture is based on the solution concept of the Traffic CS System Concept SPT2TRAFFIC-4459.

, **SP-SEC-Comp-4.2.3-1 -** The generic zone and conduits drawing for this SuC is depicted in the figure below. [Open, SPPRAMSS-9650]



, SP-SEC-Comp-4.2.3-2 - Generic Security Zoning **[** Open, SPPRAMSS-10392 **]**



, SP-SEC-Comp-4.2.3-3 - The smallest security zone is can be the Secure Component itself. The Secure Component is contained in a greater bigger zone, e.g. the OT/Signaling zone. The conduits are the interfaces to other components, the Shared Cybersecurity Services and other OT services. See also SP-SEC-Comp-4-1-3 - 1 Interfaces of the SuC **[** Open, SPPRAMSS-10407 **]**SuC .

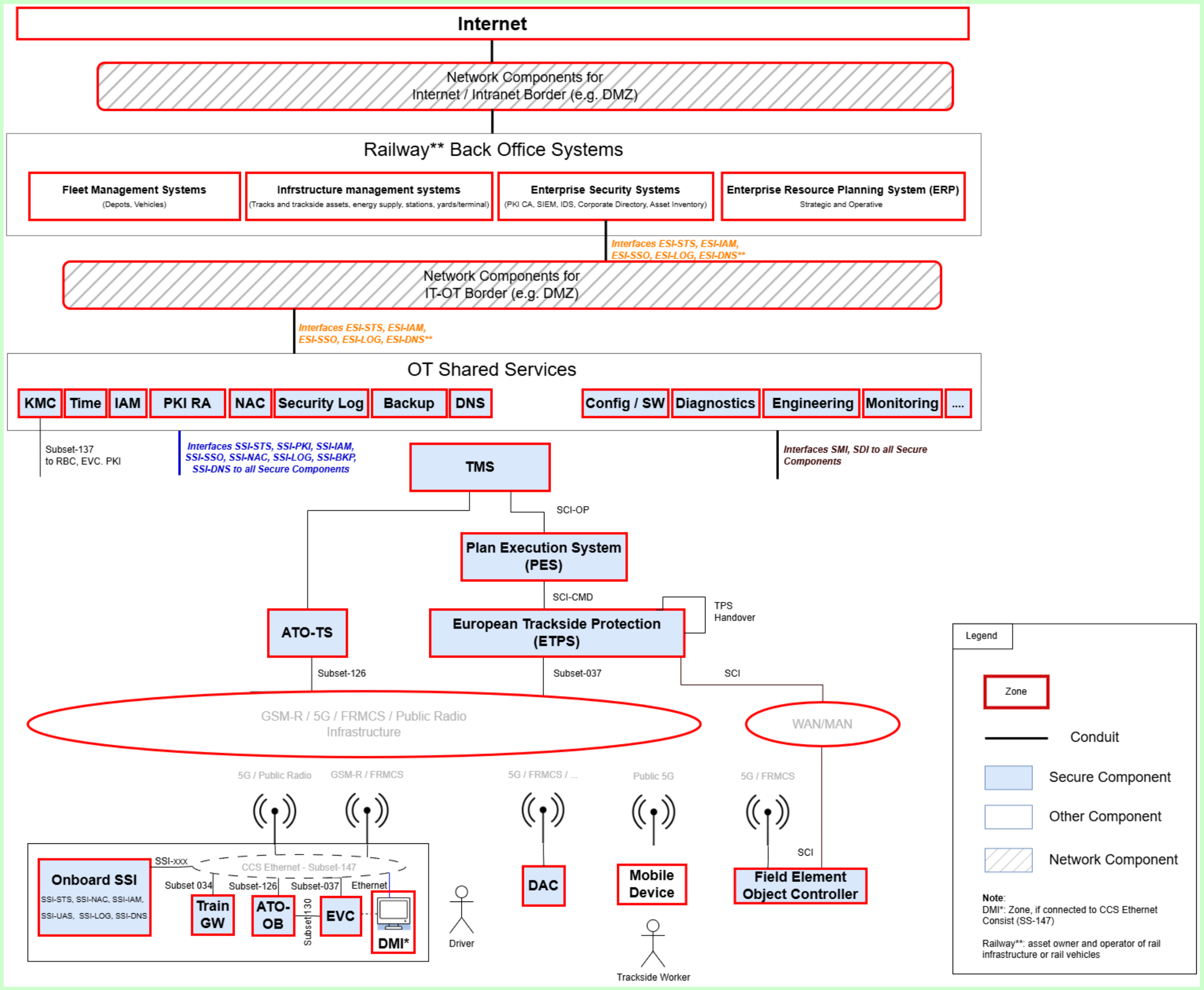
, SP-SEC-Comp-4.2.3-4 - A special security zone is the legacy component zone. In order to interface with Secure Components, as a Security Proxy implementing this specification has to can be used. As this zone uses insecure communication (i.e. communication without authentication or integrity protection), additional physical security measures are typically required. **[** Open, SPPRAMSS-10405 **]**

, SP-SEC-Comp-4.2.3-5 - Wireless devices are normally grouped in dedicated wireless security zones. In above drawing, the Secure Components have either wired and/or wireless interfaces and are in their own security zone.

, SP-SEC-Comp-4.2.3-56 - The generic zone and conduit drawing can be mapped to a specific zone and conduit drawing of a specific scope. The figure below shows the result of the mapping for a rail automation system. **[** Open, SPPRAMSS-10406 **]**

, SP-SEC-Comp-4.2.3-67 - Example of a Security Zone Zoning (rail automation system) , where each component has its own zone. Zones could also include several components, especially when the components are co-located.

[Open, SPPRAMSS-10391]


Internet
Network Components for Internet / Intranet Border (e.g. DMZ)
Railway** Back Office Systems
Fleet Management Systems
(Depots, Vehicles)
Infrstructure management systems
(Tracks and trackside assets, energy supply, stations, yards/terminal)
Enterprise Security Systems
(PKI CA, SIEM, IDS, Corporate Directory, Asset Inventory)
Enterprise Resource Planning System (ERP)
Strategic and Operative
Interfaces ESI-STS, ESI-IAM, ESI-SSO, ESI-LOG, ESI-DNS**
Network Components for IT-OT Border (e.g. DMZ)
Interfaces ESI-STS, ESI-IAM, ESI-SSO, ESI-LOG, ESI-DNS**
OT Shared Services
KMC
Time
IAM
PKI RA
NAC
Security Log
Backup
DNS
Config / SW
Diagnostics
Engineering
Monitoring
....
Subset-137 to RBC, EVC. PKI
Interfaces SSI-STS, SSI-PKI, SSI-IAM, SSI-SSO, SSI-NAC, SSI-LOG, SSI-BKP, SSI-DNS to all Secure Components
TMS
Interfaces SMI, SDI to all Secure Components
SCI-OP
Plan Execution System (PES)
SCI-CMD
TPS Handover
ATO-TS
European Trackside Protection (ETPS)
Subset-126
Subset-037
SCI
GSM-R / 5G / FRMCS / Public Radio Infrastructure
WAN/MAN
5G / Public Radio
GSM-R / FRMCS
5G / FRMCS / ...
Public 5G
5G / FRMCS
SSI-xxx
CCS Ethernet - Subset-147
Onboard SSI
SSI-STS, SSI-NAC, SSI-IAM, SSI-UAS, SSI-LOG, SSI-DNS
Subset 034
Subset-126
Subset-037
Ethernet
Train GW
ATO-OB
Subset130
EVC
DMI*
Driver
DAC
Mobile Device
Trackside Worker
SCI
Field Element Object Controller
Legend
Zone
Conduit
Secure Component
Other Component
Network Component
Note:
DMI*: Zone, if connected to CCS Ethernet Consist (SS-147)
Railway**: asset owner and operator of rail infrastructure or rail vehicles

, SP-SEC-Comp-4.2.4.1-1 - This zone description is for the security zone of the SuC (Secure Component), identified as Zone-SC. [Open, SPPRAMSS-10420]

, SP-SEC-Comp-4.2.4.2-1 - The accountable organisation for the Zone-SC is the railway duty holder. For trackside and central installed Secure Components this can be the infrastructure manager, for Secure Components installed on rolling stock the railway undertaking. [Open, SPPRAMSS-10418]wehicle owner.

, SP-SEC-Comp-4.2.4.3-1 - The logical and physical boundary of the Zone-SC in context of this specification is the encasing of the Secure Component. [Open, SPPRAMSS-10419]

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).

, **SP-SEC-Comp-4.2.4.3-2 -** The logical boundary of the Zone-SC are the logical interfaces of the Secure Component to external communication partners.

, **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. **[** Open, SPPRAMSS-10417 **]**

, **SP-SEC-Comp-4.2.4.4-2 -** Secure Components not implementing safety-related functions (e.g. components in the OT Service Zone), but interfacing with safety-related Secure Components typically have a Basic Integrity Safety Level or no Safety Level (in case non-interference can be demonstrated). **[** Open, SPPRAMSS-10421 **]**

Note: safety-related standards describing safety levels are EN 50716 and EN 50126

, **SP-SEC-Comp-4.2.4.5-1 -** The SuC has various interfaces which are described in chapter 4.1.SP-SEC-Comp-4-1-3 - Interfaces of the SuC **[** Open, SPPRAMSS-10393 **]**SuC

, **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

[Open, SPPRAMSS-10413 **]**

, **SP-SEC-Comp-4.2.4.5-3 -** Interfaces with no networking capabilities such as USB, serial, JTAG, Display Ports, removable SSD, NFC are not considered for zoning design.

, **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 propertiesprotection 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 Threat Catalog. [Open, SPPRAMSS-10398][SP-SEC-ThreatCat].

, SP-SEC-Comp-4.2.5-1 - It is assumed that a Secure Component is installed in a housing with physical access restrictions. The assumed physical security protection requirements are stated in 60_Security_Program_Requirements old. [Open, SPPRAMSS-9617]in SP-SEC-PGRM-6.2 - Physical Access Control.

, SP-SEC-Comp-4.2.5-2 - It is assumed that a Secure Component has connectivity to the shared cybersecurity services as defined in 22 Shared Cybersecurity Services Specification . [Open, SPPRAMSS-9612][SP-SEC-ServSpec] .

Note: On-board Secure Components connectivity can be intermittent. Therefore, certain Shared Cybersecurity Services should have an on-board proxy functionality (see also SP-SEC-SERV Ch. 3.2 Service Overview)

, SP-SEC-Comp-4.2.5-3 - It is assumed that the Secure Component is operated and maintained by an organization following the 60_Security_Program_Requirements old , maintained and commissioned according to the [SP-SEC-PrgmReq] , e.g. implementing [IEC 62443-2-1:2024] / [ISO/IEC 27001, and :2022] , and [IEC 62443-2-4 [Open, SPPRAMSS-9613]:2023] .

, SP-SEC-Comp-4.2.5-4 - The physical and logical environment of a specific Secure Component (in Zone-SC) is documented in chapter 5 of Secure Product Documentation [Open, SPPRAMSS-10439]of [SP-SEC-DocTempl] .

, 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. [Open, SPPRAMSS-9615]

, SP-SEC-Comp-4.2.6-2 - The threats considered for this specification are described in the Thread Catalog [Open, SPPRAMSS-10408][SP-SEC-ThreatCat].

, SP-SEC-Comp-4.2.7-1 - add reference to risk analyses

Reference to risk analysis and document result (e.g. SL-T + requirements list from 3-3, 4-2) [Open, SPPRAMSS-9609]The initial risk analysis is documented in [SP-SEC-ThreatAna]

This chapter lists the security requirements for Secure Components. The chapter is structured by technical building blocks.

Special sections are available for security requirements for specific Secure Components: Secure Components with wireless network access, Secure Components with a Human-Machine Interface (HMI), and Network Components (switches, routers, firewalls, gateways,...)

, SP-SEC-Comp-5.1-1 - The Secure Component shall be developed according to 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 practised practiced at least for one product (with required evidence). [SPPRAMSS-2495, Generic , no]

, SP-SEC-Comp-5.1-2 - The Secure Component shall use for the implementation of security functionality preferably 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). **[**SPPRAMSS-9632, Generic , no **]**

, SP-SEC-Comp-5.2.1-1 - The Secure Component shall provide an internal real-time clock.

Note: this does not require a battery-buffered clock. However, a battery- or supercapacitor-buffered clock simplifies and speeds up the time synchronization during start up (e.g. after a power cycle) and enhances the entropy for seeding the random-number generator of the operating system. **[**SPPRAMSS-3873, Generic , no **]**

, SP-SEC-Comp-5.2.1-2 - In the absence of battery-buffered clock, or exhaustion of battery capacity, the Secure Component shall maintain monotonic date and time for its real-time clock upon reboot.

Note 1: This could be achieved by periodic storage of current time during execution and reload of last known date upon reboot.
Note 2: Verification of certificate and certificate revocation list and logging of security-related events do not require a high level of accuracy, as usually +/- 1 second is acceptable. With NTP/NTS the achieved time synchronization can be improved. **[**SPPRAMSS-7462, Generic , no **]**

, SP-SEC-Comp-5.2.2-1 - A Secure Component should follow the guidance for initializing random numbers with sufficient entropy by following the recommendations in in [RFC - 4086]. **[**SPPRAMSS-9665, Generic , no **]**

, 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. **[**SPPRAMSS-2941, Generic , no **]**

, 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). **[**SPPRAMSS-3099, Generic , no **]**

, SP-SEC-Comp-5.2.4-1 - The Secure Component shall support the update of the firmware of security-related hardware mechanisms.

Note: Examples of firmware of secure hardware mechanism include secure boot functions, firmware of trusted environments, UEFI. **[**SPPRAMSS-3102, Generic , no **]**

, SP-SEC-Comp-5.2.5-1 - The Secure Component shall use the Secure Boot functions defined by the used chipset manufacturer. **[**SPPRAMSS-3105, Generic , no **]**

, SP-SEC-Comp-5.2.5-2 - The Secure Component shall use the certificate chain up to the Manufacturer Root CA Certificate (MRCAC) (refer to SPPRAMSS-5650SP-SEC-ServSpec Ch 5.2.1 - Manufacturer Certificates) to verify the authenticity of the firmware, boot-loader and operating system.

Note: If the Secure Component uses a COTS hardware provided by a 3rd party, the existing credentials (e.g. Microsoft keys in UEFI) can be used as the Manufacturer Root CA Certificate (MRCAC) to verify the authenticity of the firmware, boot-loader and operating system. Additional risks created needs to be analysed and documented. **[**SPPRAMSS-6577, Generic , no

Note: If the Secure Component is an embedded systems, the first stage of Secure Boot uses different credentials (e.g. write-once keys or hashes) defined by the used chipset manufacturer and not the MRCAC. **[**Generic **]**

, SP-SEC-Comp-5.2.5-3 - If a secure boot verification fails, the Secure Component shall provide a visible or audible indication.

Note: the visual or audible indication of an integrity check failure is necessary, as the Secure Component cannot securely log anything errors before successful start-up of the operating system is completed. 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 **[**SPPRAMSS-3429, Generic , no **]**

, 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. **[**SPPRAMSS-2473, Generic , no **]**

, 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. **[**SPPRAMSS-3729, Generic , no **]**

, 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. **[**SPPRAMSS-4911, Generic , no **]**

, SP-SEC-Comp-5.2.5-7 - Note: Examples of secure boot stages are chipset, BIOS/UEFI, boot loader, operating system. **[** Open, SPPRAMSS-3108 **]**

, SP-SEC-Comp-5.2.6-1 - When powered the Secure Component shall provide a tamper detection mechanism which detects the opening of the physical encasing. **[**SPPRAMSS-3111, Generic , no **]**

, SP-SEC-Comp-5.2.6-2 - If tampering is detected, the Secure Component shall provide notification of the detection to the SSI-LOG service.
Note: If a Secure Component does not implement these functions, then the environment where the Secure Component is installed needs to provide these functions (e.g. tamper-protected cabinet). See also chapter 3.5 how to document and export not implemented requirements (e.g. as security application condition as access-controlled environment with tamper detection and alarm function e.g. room). **[**SPPRAMSS-3110, Generic , no **]**

, SP-SEC-Comp-5.2.7-1 - The supplier shall provide a security seal on the Secure Component. **[**SPPRAMSS-2994, Generic , no **]**

, SP-SEC-Comp-5.2.7-2 - The security seal shall contain a number unique to the supplier. **[**SPPRAMSS-2998, Generic , no **]**

, SP-SEC-Comp-5.2.7-3 - The supplier shall place the security seal on the enclosure edges which breaks the seal, if the enclosure is opened. **[**SPPRAMSS-2634, Generic , no

Note: seals should not be placed on edges which are opened for operation (e.g laptop screen vs. laptop housing, access panel for regular maintenance vs. internal interfaces) **[**Generic **]**

, SP-SEC-Comp-5.2.7-4 - The seals shall be designed to break in case of standard attacks using heat or solvents. **[**SPPRAMSS-2637, Generic , no **]**

, SP-SEC-Comp-5.2.8-1 - The Secure Component shall bear a type, batch or serial number on its enclosure. **[**Generic **]**

, SP-SEC-Comp-5.2.89-1 - 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. **[**SPPRAMSS-6695, Generic , no **]**

, SP-SEC-Comp-5.2.910-1 - The Secure Component should be designed with crypto agility in mind. It is envisonedenvisioned, that during the lifetime of a Secure Component, additional ciphers are added to a future version of these specifications (e.g. to support post quantum cryptography). This requires to update firmware of the component, update of issued certificates (e.g. MDC, ODC,..), use of new ciphers or a combination of ciphers for protecting communication and ensuring integrity of files (e.g. configuration files, CMP messages) and additional certificate profiles. The hardware specification (especially for CPU and memory specs) should envision these upcoming changes. [Open, SPPRAMSS-10110]

, SP-SEC-Comp-5.3.1-1 - The Secure Component shall use a process allowlist to protect against execution of unauthorised software.
Note: an allowlist typically contains the hashes of the authorised executable binaries. [SPPRAMSS-3425, Generic , no]

, SP-SEC-Comp-5.3.1-21 - The Secure Component shall only start a software process if it is part of the allowlist. [SPPRAMSS-3015, Generic , no 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. [Generic]

, SP-SEC-Comp-5.3.1-32 - At startup, the Secure Component shall check the integrity and authenticity of the allowlistruntime integrity check.
Note: if the allowlist could 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. [SPPRAMSS-3720, Generic , no]

, 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. [SPPRAMSS-2471, Generic , no]

, 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. [SPPRAMSS-2488, Generic , no]

, SP-SEC-Comp-5.3.2-3 - If a Secure Component is implementing a Juridical Recording function, then it shall protect the integrity of juridical recording data at rest. [SPPRAMSS-2493, Generic , no

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

, 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. [SPPRAMSS-3013, Generic , no]

, 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. [SPPRAMSS-3023, Generic , no]

, 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.8 [SPPRAMSS-3022, Generic , yes]

, SP-SEC-Comp-5.3.5-2 - The supplier shall document the predetermined state for Secure Component with physical I/O (e.g. the safe state). [SPPRAMSS-4998, Generic , no]

, SP-SEC-Comp-5.3.6-1 - The Secure Component shall implement the hardening measures according to the relevant **[CIS benchmark]**, achieving compliance to at least Level 1 or in accordance with a comparable benchmark and compliance level. [SPPRAMSS-3779, Generic , no]

, 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). [SPPRAMSS-2301, Generic , no]

, SP-SEC-Comp-5.3.7-2 - The Secure Component shall update its internal real-time clock with the synchronized time received via [via interface SSI-STS](refer to SP-SEC-ServSpec Ch 4 - STS: Secure Time Synchronisation). [SPPRAMSS-7524, Generic , no]

, SP-SEC-Comp-5.4.1-1 - The Secure Component shall support **[IEEE 802.1Q-2018]** tagged VLAN and multiple gateways (at least one per IP network used).
Note: this allows logical network segmentation for zone and conduits. [SPPRAMSS-2543, Generic , no]

, SP-SEC-Comp-5.4.1-2 - The Secure Component shall be capable to bind each communicating process to configured interface(s) corresponding to a specific VLAN. [SPPRAMSS-7526, Generic , no]

, SP-SEC-Comp-5.4.1-3 - The Secure Component shall 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. [SPPRAMSS-7528, Generic , no]

, 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). [SPPRAMSS-3822, Generic , no]

, 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. [SPPRAMSS-3821, Generic , no]

, 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. [SPPRAMSS-2555, Generic , no]

, SP-SEC-Comp-5.4.2-4 - If the Secure Component supports packet forwarding, the Secure Component's host-based firewall filter shall be capable of filtering forwarded network traffic. [SPPRAMSS-7529, Generic , no]

, SP-SEC-Comp-5.4.3-1 - The Secure Component shall support to authenticate to the network using the SSI-NAC interface (see Shared Cybersecurity Services Spec - 8. SSI-NAC interfacerefer to SP-SEC-ServSpec Ch 7 - NAC: Network Access Control). [SPPRAMSS-2315, Generic , no]

, SP-SEC-Comp-5.4.3-2 - The Secure Component shall support separate re-authentication per physical network interface using NAC. [SPPRAMSS-2317, Generic , yes]

, **SP-SEC-Comp-5.4.3-3 -** The Secure Component shall use the Operator Device Certificate (ODC) as specified in50_Shared Security Services - SP-SEC-ServSpec Ch 13.1.2-1 - Operator Device Certificate (ODC) profile for authentication towards the Network Authentication Server. **[**SPPRAMSS-4892, Generic , no **]**

, **SP-SEC-Comp-5.4.3-4 -** If no Operator Device Certificate (ODC) is available, the Secure component shall use the Manufacturer Device Certificate (MDC) as specified in 50_Shared Security Spec - SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile for for authentication towards the Network Authentication Server.
Note: to ensure that the Network Authentication Server uses the Manufacturer Device Certificate (MDC) only in the cases where it is necessary (e.g. when a new device is plugged into the network which does not have an Operator Root CA Certificate), the Network Authentication Server will authenticate itself by picking the certificate based on the EAP identity sent by the supplicant.
[SPPRAMSS-4891, Generic , no **]**

, **SP-SEC-Comp-5.4.3-5 -** If the Secure Component has no Operator Root CA Certificate (ORCAC) available, the Secure Component shall use the EAP identity "manufacturer". **[**SPPRAMSS-4894, Generic , no

Note: in this case, the Secure Component uses the MRCAC (initial commissioning phase) **[**Generic **]**

, **SP-SEC-Comp-5.4.3-6 -** If the Secure Component has an Operator Root CA Certificate (ORCAC) available, the Secure Component shall use the EAP identity "operator". **[**SPPRAMSS-4893, Generic , no **]**

, **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 situation situations over an extended period of time. The test should show that resource utilization stays in the specified limits. **[**SPPRAMSS-9633, Generic , yes **]**

, **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 SPPRAMSS-2630 and SPPRAMSS-9633 **[**SPPRAMSS-3781, Generic , yes SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1 **[**Generic **]**

, **SP-SEC-Comp-5.4.4-3 -** The Secure Component shall use the interfaces defined in this specification, the Secure Communication Specification and Shared Cybersecurity Specification or if an additional interface is used, implement the requirements from SPPRAMSS-6667 - Components with additional communicating processes .
Note: This reduces the effects of an Denial of Service attack, since all interfaces require authentication. **[**SPPRAMSS-9750, Generic , no **]**

, **SP-SEC-Comp-5.4.4-43 -** 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). **[**SPPRAMSS-2630, Generic , yes **]**

, **SP-SEC-Comp-5.4.5.1-1 -** The Secure Component shall be capable of utilizing a unique X.509 v3 certificate as defined in RFC 5280 for each of its communicating software processes. **[**SPPRAMSS-2967, Generic , no **]**

, **SP-SEC-Comp-5.5.1-2 -** The Secure Component shall authenticate each communication partner by validating the partner's certificate in accordance with chapter SPPRAMSS-6678 - PKI Certificate Validation . **[**SPPRAMSS-3999, Generic , no 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'). **[**Generic **]**

, SP-SEC-Comp-5.5.21-1 - If the Secure Component uses the standard communication protocols defined in 21 Secure Communication Specification [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the 21 Secure Communication Specification [SP-SEC-CommSpec]. **[**SPPRAMSS-6676, Generic , no **]**

, SP-SEC-Comp-5.5.21-2 - The Secure Component shall implement the interfaces defined in 22 Shared Cybersecurity Services Specification [SP-SEC-ServSpec].

Note: 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 chapter ☐ SPPRAMSS-6667 **[**SPPRAMSS-6675, Generic , no 7 of [SP-SEC-CommSpec] **[**Generic **]**

, SP-SEC-Comp-5.5.2-3 - The Secure Component shall use the interface **[SSI-IAM]** in order to retrieve the permissions for a specified user (human or technical user) via the IAM.

Note: this is applicable for diagnostic communication and additional communication interfaces (e.g. Webserver, FTP, SSH,...), but not applicable for safety-relevant communication / M2M communication. **[**SPPRAMSS-2310, Generic , no **]**

, SP-SEC-Comp-5.5.2-4 - The Secure Component shall enforce access based on retrieved permissions for all diagnostic, maintenance and administration communication interfaces.

Note: in cases of no network availability or no access to an IAM service instance, the Secure Component should fall back on a default or configurable permission list residing on the component. **[**SPPRAMSS-2311, Generic , no **]**

, SP-SEC-Comp-5.5.32-1 - The Secure Component shall implement the interface SPPRAMSSSP-1496 - PKI: SEC-ServSpec Ch 5 - Public Key Infrastructure to to request certificates. **[**SPPRAMSS-2324, Generic , no **]**

, SP-SEC-Comp-5.5.32-2 - The Secure Component shall generate a new individual key pair for every requested certificate. **[**SPPRAMSS-4180, Generic , no **]**

, SP-SEC-Comp-5.5.32-3 - The Secure Component shall generate keys on the Secure Component itself. **[**SPPRAMSS-2509, Generic , no **]**

, SP-SEC-Comp-5.5.32-4 - The Secure Component shall implement the interfaces SPPRAMSSSP-1496SEC-ServSpec Ch 5 - PKI: Public Key Infrastructure to renew a certificate. **[**SPPRAMSS-2322, Generic , no **]**

, SP-SEC-Comp-5.5.32-5 - 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. **[**SPPRAMSS-2335, Generic , yes **]**

, SP-SEC-Comp-5.5.32-6 - If the certificate update contains a renewed certificate which is used in current communication, the Secure Component shall re-establish the communication using the renewed certificate. **[**SPPRAMSS-10125, Generic , no **]**

, SP-SEC-Comp-5.5.32-7 - If the renewed certificate(s) corresponds to a two-channel safety-related connection (e.g. SCI), the Secure Component shall re-establish communications only one active channel at a time.

Note: If in a two-channel safety communication, one channel is not active (e.g. in maintenance, not connected), a diagnostic event should be generated and the re-establishment should happen when the other channel becomes active again. **[**SPPRAMSS-4379, Generic , yes **]**

, SP-SEC-Comp-5.5.32-8 - The Secure Component shall be able to support trust a list of certificate authorities.

Note: a PKI hierarchy can have multiple trusted certificate authorities (manufacturer and several operators). [SPPRAMSS-2428, Generic , no]

, SP-SEC-Comp-5.5.32-9 - The Secure Component shall update its CRLs as defined in RFC 5280 chapter 6.3.3.

Note: a diagnostic method is also available to trigger a CRL update when required. See chapter 5.7.2 (SPPRAMSS-2336) [SPPRAMSS-2437, Generic , no via the SSI-PKI interface. [Generic]

, SP-SEC-Comp-5.5.2-10 - The Secure Component shall update its CRLs as defined in RFC 5280 chapter 6.3.3 or by using externally configured CRL distribution points.

Note: a diagnostic method is also available to trigger a CRL update when required. See SP-SEC-Serv-12.2-1 [Generic]

, SP-SEC-Comp-5.5.32-1011 - If the Secure Component cannot fetch a new CRL after the time defined by the nextUpdate field, the Secure Component shall keep using the latest locally cached CRL. [SPPRAMSS-8039, Generic , no]

, SP-SEC-Comp-5.5.32-1112 - If an CRL update contains certificate which is used in current communications, the Secure Component shall terminate the communications using the revoked certificate. [SPPRAMSS-10124, Generic , yes]

, SP-SEC-Comp-5.5.32-1213 - The Secure Component shall support certificates defined in the SPPRAMSSSP-5087 - Use Case: Updating Operator Certificates . [SPPRAMSS-2435, Generic , no SEC-ServSpec Ch 13.1 - Certificate Profiles . [Generic]

, SP-SEC-Comp-5.5.43-1 - The Secure Component shall check if the certificate signature is valid. [SPPRAMSS-6679, Generic , no]

, SP-SEC-Comp-5.5.43-2 - The Secure Component shall validate the certificate's trust chain up to a trusted certificate authority. [SPPRAMSS-2432, Generic , no]

, SP-SEC-Comp-5.5.43-3 - The Secure Component shall check if the certificate is not revoked using CRLs. [SPPRAMSS-2431, Generic , no]

, SP-SEC-Comp-5.5.43-4 - If the lifetime of the certificate is not valid when checking the notBefore and notAfter certificate fields against the current time and date, the Secure Component shall reject the certificate or issue an diagnostic alarm depending on its configuration. [SPPRAMSS-7579, Generic , no]

, SP-SEC-Comp-5.5.43-5 - The Secure Component shall check if the communication partner has control of the private key corresponding to the presented certificate.

Note: Control of the private key by communication partner is normally implemented in challenge-response mechanisms. Examples of implementation is TLS, and for both communication parties: TLS mutual authentication. [SPPRAMSS-6659, Generic , no]

, SP-SEC-Comp-5.5.43-6 - The Secure Component shall map the authenticated identity of a certificate to a user (human or technical user) [SPPRAMSS-6660, Generic , no]

, SP-SEC-Comp-5.5.43-7 - The Secure Component shall validate and enforce the extended key usage according to the definition in .Shared Cybersecurity Specification SPPRAMSS-5125 - OID Overview [SPPRAMSS-9989, Generic , no SP-SEC-ServSpec Ch 5.2-3 - Object Identifiers (OIDs) [Generic]

, SP-SEC-Comp-5.5.43-8 - If the Secure Component cannot validate certificates because of a missing secure time

source (e.g. during initial comissioningcommissioning), the Secure Component shall use a fallback time source.
Note: The fallback time can for example be calcaluted calculated using the following (possibly non-secure) time sources: NTP, earliest permissble time from 'Not Before' field from Manufacturer Device Certificate (MDC)last shutdown time, real-time clock of the device. **[**SPPRAMSS-7967, [Component Type], [Requirements supports essential function] **]**Generic **]**

, **SP-SEC-Comp-5.5.54-1 -** 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 Shared Cybersecurity Specification SPPRAMSS-7641 - SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile . **[**SPPRAMSS-4960, Generic , no **]**

, **SP-SEC-Comp-5.5.54-2 -** The corresponding private key of the MDC shall be either generated on the device upon either production or commissioning. **[**SPPRAMSS-7582, Generic , no **]**

, **SP-SEC-Comp-5.5.54-3 -** The certificate chain of the MDC up required to the corresponding root-of-trust validate the certificate shall be installed on the device upon production or commissioning (see also SPPRAMSSSP-4967 - The Secure Component shall have the capability to install trusted certificates i... SEC-CompSpec Ch 5.5.5.-1). **[**SPPRAMSS-7583, Generic , no **]**

, **SP-SEC-Comp-5.5.54-4 -** The Secure Component shall have the capability to install and remove Operator Root CA Certificates (ORCACs)

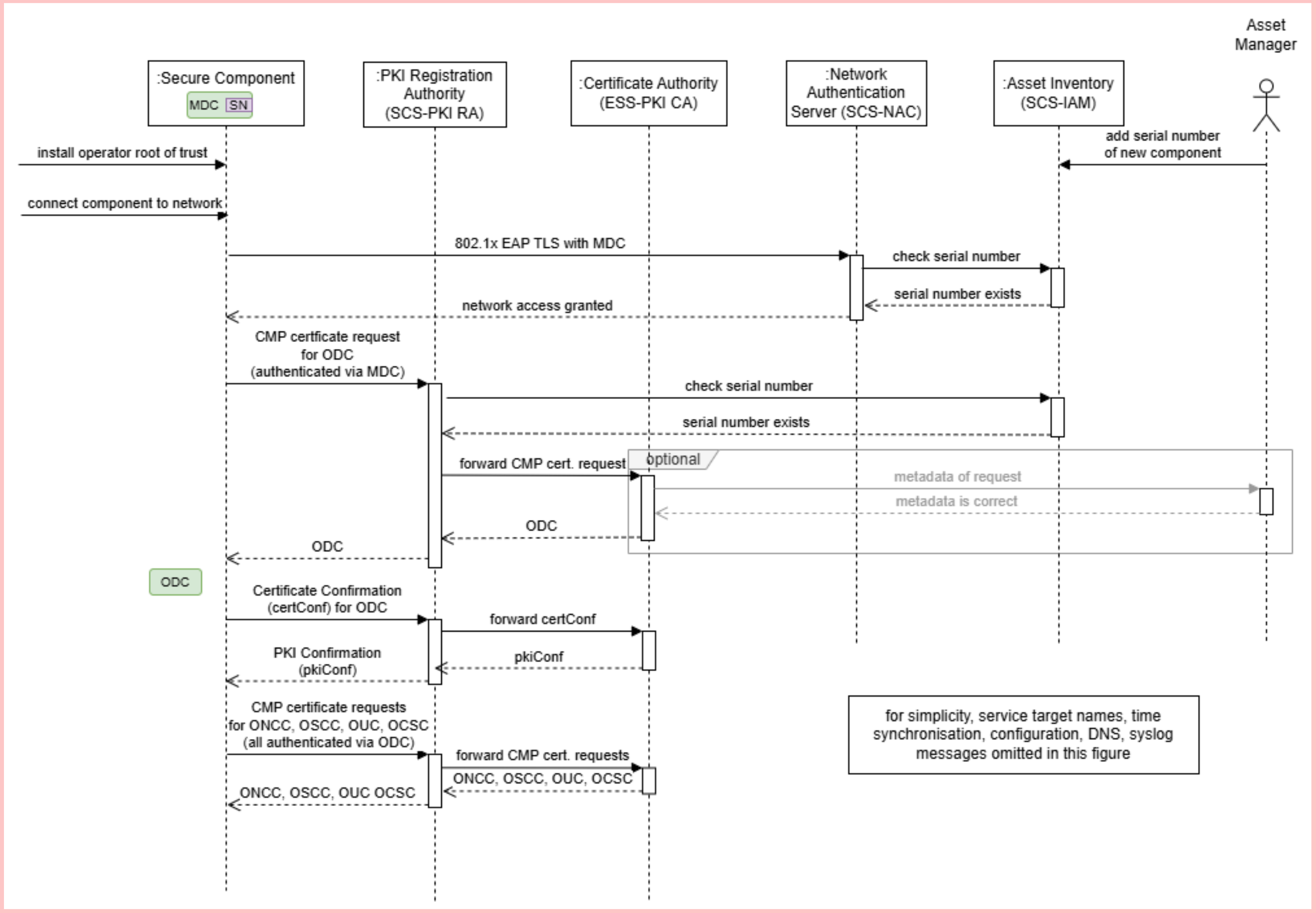
that that are defined in a configuration file signed by the Manufacturer Trust Anchor Signer Certificate (MTASC) or Operator Trust Anchor Signer Certificate (OTASC) during the commissioning phase or earlier.

[SPPRAMSS-7597, Generic , no **]**

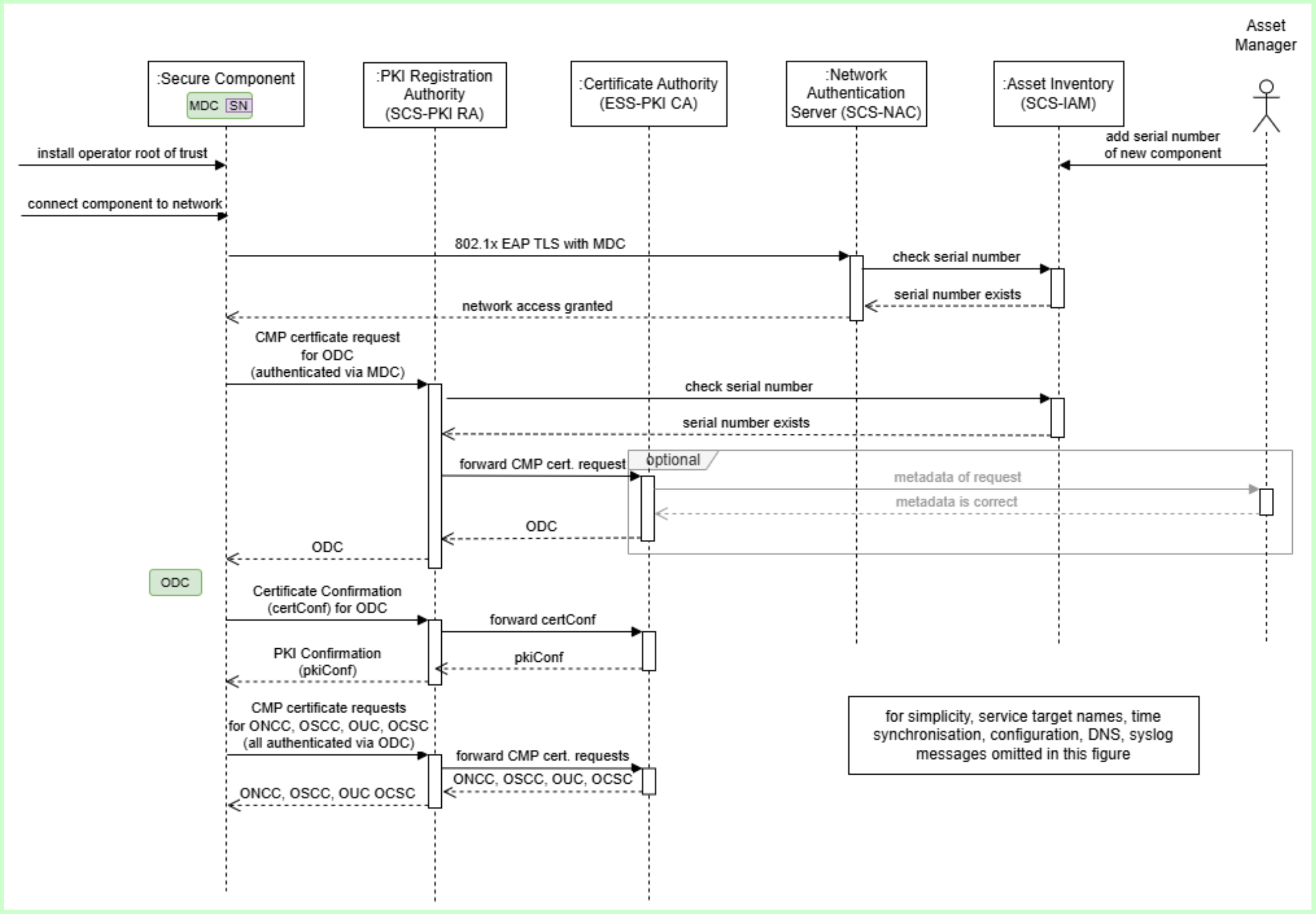
, **SP-SEC-Comp-5.5.5-5 -** If no ODC is available, the Secure Component shall request network access via the SSI-NAC interface using the Manufacturer Device Certificate (MDC) for authentication. **[**SPPRAMSS-4963, Generic , no **]**

, **SP-SEC-Comp-5.5.4-5 -6 -** The Secure Component shall request the Operator Device Certificate (ODC) via the SSI-PKI interface using the Manufacturer Device Certificate (MDC) for message protection. **[**SPPRAMSS-4961, Generic , no **]**

, **SP-SEC-Comp-5.5.54-76 -** The Secure Component shall request all other operator certificates (ONCC, OSCC, OUC, OCSC, see SPPRAMSSSP-5087 - 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. **[**SPPRAMSS-4962, Generic , no **]**


Asset Manager
:Secure Component
MDC
SN
:PKI Registration Authority (SCS-PKI RA)
:Certificate Authority (ESS-PKI CA)
:Network Authentication Server (SCS-NAC)
:Asset Inventory (SCS-IAM)
add serial number of new component
install operator root of trust
connect component to network
802.1x EAP TLS with MDC
check serial number
serial number exists
network access granted
CMP certficate request for ODC (authenticated via MDC)
check serial number
serial number exists
forward CMP cert. request
optional
metadata of request
metadata is correct
ODC
ODC
ODC
Certificate Confirmation (certConf) for ODC
forward certConf
PKI Confirmation (pkiConf)
pkiConf
CMP certificate requests for ONCC, OSCC, OUC, OCSC (all authenticated via ODC)
forward CMP cert. requests
ONCC, OSCC, OUC, OCSC
ONCC, OSCC, OUC OCSC
for simplicity, service target names, time synchronisation, configuration, DNS, syslog messages omitted in this figure

, **SP-SEC-Comp-5.5.4-7 -** Overview of commissioning steps:


Asset Manager
:Secure Component
MDC
SN
:PKI Registration Authority (SCS-PKI RA)
:Certificate Authority (ESS-PKI CA)
:Network Authentication Server (SCS-NAC)
:Asset Inventory (SCS-IAM)
add serial number of new component
install operator root of trust
connect component to network
802.1x EAP TLS with MDC
check serial number
serial number exists
network access granted
CMP certficate request for ODC (authenticated via MDC)
check serial number
serial number exists
forward CMP cert. request
optional
metadata of request
metadata is correct
ODC
ODC
ODC
Certificate Confirmation (certConf) for ODC
forward certConf
PKI Confirmation (pkiConf)
pkiConf
CMP certificate requests for ONCC, OSCC, OUC, OCSC (all authenticated via ODC)
forward CMP cert. requests
ONCC, OSCC, OUC, OCSC
ONCC, OSCC, OUC OCSC
for simplicity, service target names, time synchronisation, configuration, DNS, syslog messages omitted in this figure

, **SP-SEC-Comp-5.5.54-8 -** Note: for validation and testing purposes there might be additional certificate types used. **[** Open, SPPRAMSS-7581 **]**

, SP-SEC-Comp-5.5.54-9 - Note: the step of checking additional metadata before issuing certificates is optional. The operator may define metadata to be checked. **[** Open, SPPRAMSS-9941 **]**

, SP-SEC-Comp-5.5.54-10 - Note: usage of different networks for commissioning is optional and not depicted in the drawing. **[** Open, SPPRAMSS-9991 **]**

, SP-SEC-Comp-5.5.65-1 - 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 . **[**SPPRAMSS-4967, Generic , no **]**

, SP-SEC-Comp-5.5.65-2 -

The Secure Component shall have the capability to install certificate chains in the certificate store via the mechanism described in Chapter SP-SEC-CompSpec Ch 5.6.1 - Software Update . **[**SPPRAMSS-8898, Generic , no **]**

, SP-SEC-Comp-5.6.1-1 - The Secure Component shall support the update of software and configuration via the interface (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. **[**SPPRAMSS-2497, Generic , yes **]**

, SP-SEC-Comp-5.6.1-2 - The Secure Component shall provide the ability to update the non-safety related software and configuration without affecting existing safety approvals. **[**SPPRAMSS-2503, Generic , no shall ensure that the safety functionality is not influenced by the security functionality.

Note: this ensures that security updates can be installed without affecting safety certifications. This can be achieved i.e. by demonstrating non-interference between safety and security functionality. Technical measures to ensure non-interference are logical separation and protection of computer resources.

[Generic **]**

, 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. **[**SPPRAMSS-2982, Generic , no **]**

, SP-SEC-Comp-5.6.1-4 - The Secure Component shall reject update packages without a valid signature. **[**SPPRAMSS-2984, Generic , no **]**

Note: This chapter is for the SMI update package (used for reference from SMI specification)

, SP-SEC-Comp-5.6.2-1 - The update package shall be signed using the corresponding update signing key (corresponding to MUSC and OUSC). **[**SPPRAMSS-4028, Generic , no .

Note: the corresponding update signing key for firmware update is the MUSC and for configuration update is the MCSC or OCSC. **[**Generic **]**

, SP-SEC-Comp-5.6.2-2 - The update package shall use SHA-512 hash algorithm for the integrity protection. **[**SPPRAMSS-2498, Generic , no **]**

, SP-SEC-Comp-5.6.2-3 - The update package shall use X.509v3 certificates including extended key usage code signing for
the update package signature. **[**SPPRAMSS-2989, Generic , no **]**

, 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 SPPRAMSS-1490 - 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. **[**SPPRAMSS-3078, Generic , no **]**

, 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 SPPRAMSSSP-1490SEC-ServSpec Ch 11 - BKP: Backup and Restore **[**SPPRAMSS-6750, Generic , no **]**

, 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 SPPRAMSSSP-1490SEC-ServSpec Ch 11 - BKP: Backup and Restore **[**SPPRAMSS-6749, Generic , no **]**

Security Logging contains the continuous stream of logging events from operating systems and applications from a Secure Component. In contrast, Security Diagnostic contains the current state of the Secure Component, based on a diagnostics model.

, SP-SEC-Comp-5.7.1-1 - The Secure Component 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). **[**SPPRAMSS-2581, Generic , no

Note: more detail of log events is described in chapter SP-SEC-ServSpec Ch 9.1 - Log Message Format **[**Generic **]**

, SP-SEC-Comp-5.7.1-2 - The Secure Component shall send the logging events via SSI-LOG SPPRAMSSSP-1489SEC-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. **[**SPPRAMSS-2580, Generic , no **]**

, SP-SEC-Comp-5.7.1-3 - The Secure Component shall provide the capability to send logging data to multiple configurable log collector destinations. **[**SPPRAMSS-4407, Generic , no **]**

, SP-SEC-Comp-5.7.1-4 - The Secure Component shall send log messages complying to the log message format defined in SPPRAMSSSP-3869 - 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 **[**SPPRAMSS-2588, Generic , no **]**

, SP-SEC-Comp-5.7.1-5 - 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 chapter 5.7.2.3in SP-SEC-Serv Ch 12.3 - Log Maintenance . The untransferred logs are assumed to be accessible until a restart / reboot.

[SPPRAMSS-2598, Generic , no **]**

, SP-SEC-Comp-5.7.1-6 - The Secure Component implementing a Log Server (ie.e g. a Log Relay) shall store log data on a non-volatile memory for a configurable duration.

Note: typical log retention duration depend on the log destination retention capabilities (e.g. SIEM features) and network connectivity. In mobile environments (e.g a train), a log server / relay in the mobile environment with longer retention duration may be required. **[**SPPRAMSS-2597, Generic , no **]**

, SP-SEC-Comp-5.7.1-7 - If the storage capacity is exceeded, the Secure Component shall overwrite the oldest log entry first. **[**SPPRAMSS-2596, Generic , yes **]**

, SP-SEC-Comp-5.7.1-8 - 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. **[**SPPRAMSS-3070, Generic , no **]**

, SP-SEC-Comp-5.7.1-9 - If the Secure Component starts overwriting not transferred log data, it shall generate a log that overwriting has started. **[**SPPRAMSS-4439, Generic , no **]**

The following security maintenance method and diagnostic value definitions should be implemented using the protocols defined in SDI.

, SP-SEC-Comp-5.7.2.1-1 - The Secure Component shall provide the diagnostic value Security:SecurityStatus (Boolean) to represent the overall security status of the component.

Note: the value is TRUE when no security related issues (expired certificates, integrity errors, availbility errors to SSI, are currently present, , the value is FALSE when security issues are currently present. **[**SPPRAMSS-10127, Generic , no **]**

, SP-SEC-Comp-5.7.2.1-2 - The Secure Component shall provide the diagnostic value Security:IntegrityCheckStatus (Boolean) to represent the status of the integrity checks.

Note: the value is TRUE when no integrity failures have been reported (process allowlist checks, signature checks for files,...) and FALSE when integrity errors have occured since boot time. Details of errors is available from the security logs. **[**SPPRAMSS-10126, Generic , no **]**

, SP-SEC-Comp-5.7.2.2-1 - The Secure Component shall provide the maintenance method Security:UpdateRevocationsLists() to request the update of the CRLs.

Note: if a CRL update contains a revoked certificate used in current communication, the communication has to be terminated (see SPPRAMSS-10124).

[SPPRAMSS-2336, Generic , no **]**

, SP-SEC-Comp-5.7.2.2-2 - The Secure Component shall provide the maintenance method Security:RenewCert(String certID) to renew its certificates.

Note 1: The default method for certificate renewal is done automatically via SSI-PKI interface automatically. The diagnostic method covers edge cases when certificate renewal is necessary before certificate expiration.

Note 2: If the renewed certificate is used in current communication, the communication has to be re-established (see SPPRAMSS-10125). **[**SPPRAMSS-4381, Generic , no **]**

, **SP-SEC-Comp-5.7.2.2-3 -** The Secure Component shall provide the maintenance method Security:GetInstalledCerts() (File/String) to obtain the public certificates available on the Secure Component as String / GZIP file (RFC 1952).

Note: the return value is a compressed file containing all public certificates available on the Secure Component in GZIP file format (RFC 1952). **[**SPPRAMSS-10138, Generic , no **]**

, **SP-SEC-Comp-5.7.2.2-4 -** The Secure Component shall provide the maintenance method Security:GetInstalledTrustAnchors() (String) to obtain a list of installed trusted certificates (trust root / intermediate certificates).

Note: the return value is a compressed file containing the installed and trusted certificates (trust anchors / root certificates). **[**SPPRAMSS-10139, Generic , no **]**

, **SP-SEC-Comp-5.7.2.3-1 -** The Secure Component shall provide the mainteance 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. **[**SPPRAMSS-4203, Generic , [Requirements supports essential function] **]**

, **SP-SEC-Comp-5.7.2.3-2 -** The Secure Component shall provide the diagnostic value Security:LogSize (Int32) to represent the size of the log in MBytes. **[**SPPRAMSS-10134, Generic , no **]**

, **SP-SEC-Comp-5.7.2.4-1 -** The Secure Component shall provide the maintenance method Security:GetComponentConfiguration() (String) to return the list of configuration identifiers with corresponding SHA-512 hashes.

Note 1: this maintenance method returns a comma separated list of configurations identifiers with the corresponding SHA-512 hash. Component identifiers and hashes are separated by the character '#'.

Note 2: this maintenance method can be used to detect changes in component configuration by comparing the result with previously stored configurations (or hashes). **[**SPPRAMSS-10141, Generic , no **]**

, **SP-SEC-Comp-5.7.2.4-2 -** The Secure Component shall provide the maintenance method Security:GetNetworkConfiguration() (String) to allow the network configuration properties being retrieved.

Note: this diagnostic method can be used to detect changes in network configuration by comparing the result with previously stored configurations (or hashes). **[**SPPRAMSS-3088, Generic , no **]**

, **SP-SEC-Comp-5.7.2.5-1 -** The Secure Component shall provide the maintenance method Security:FactoryReset() to purge persistent data to reset the component to factory state.

Note 1: this method can be used as part of a decommissioning process SP-SEC-PGM 10.2 Decommissioning

Note 2: this method does not purge the factory key material (e.g. the MDC together with its root certificates will stay on the devices.

Note 3: this provides the user with the ability to erase data which requires confidentiality from persistent memory. **[**SPPRAMSS-6748, Generic , yes **]**

, **SP-SEC-Comp-5.7.2.6-1 -** The Secure Component shall provide the maintenance method Security:TestProcessAllowListing() to test the functionality of the process allowlist.

Note: a typical implementation is to have an executable file with no functionality not in the allowlist (however still integrity protected, e.g. by secure boot), which is executed by this maintenance method. This triggers the allowlist 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). **[**SPPRAMSS-10142, Generic , no **]**

, **SP-SEC-Comp-5.7.2.6-2 -** The Secure Component shall provide the maintenance method Security:TestHostFirewall() to test the functionality of the host-based firewall.

Note: a typical implementation is to have a process with tries to open a connection when this maintenance method is called to a destination and port which is not in the firewall allowlist . This triggers a block of the firewall and issues a log message, which can be used to verify the security functionality of the host-based firewall. **[**SPPRAMSS-10143, Generic , no **]10 -** If the Secure Component cannot send log messages due to connection loss, caching of log messages can be used before sending the cached messages to the configured relay after the connection is reestablished.

, **SP-SEC-Comp-5.7.2.6-31 -** The Secure Component supports the verification of the intended operation of security functions by the diagnostic values and maintenance methods in this chapter.

Security Function	Verification	Verification time
Process Allowlisting	maintenance call Security:TestProcessAllowListing()	during normal operation
Security Logging	implicit tested via Security:TestProcessAllowListing() which produces a log message	during normal operation
Integrity checks	maintenance call Security:IntegrityCheckStatus()	during normal operation
Certificates Management	maintenance call Security:GetInstalledCerts(), Security:GetInstalledCRLs() and Security:RenewCert()	during normal operation
Hardware trust anchor	only postive only positive test case: maintenance call Security:GetInstalledCerts(), Security:GetInstalledRoots()	during normal operation
Host-based firewall	maintenance call Security: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 reacts on maintenance calls (e.g. Security:SecurityStatus()	during normal operation
Network Access control	only positive test case: Secure Component has successfully connected to the network and reacts on maintenance calls (e.g. Security:SecurityStatus()	during normal operation

Security Function	Verification	Verification time
Identification and Authentification Authentication	any call to the maintenance interface involves user idententification identification and authentificationauthentication, 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
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

[Open, SPPRAMSS-3010 **]**

, 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 (MRCAC).
Note: the Manufacturer Device Certificate (MDC) plays a role in the commissioning identification/authentication/security bootstrapping process, and software/firmware updates. **[**SPPRAMSS-2308, Generic , no **]**

, SP-SEC-Comp-6.1-2 - The Secure Component encasing shall include the type, batch, version or serial number or other element allowing the identification of the corresponding Secure Component. **[**SPPRAMSS-6895, Generic , no **]**

, SP-SEC-Comp-6.2-1 - The Secure Component shall support the SMI interface for updating the security configuration. **[**SPPRAMSS-3086, Generic , no **]**

, SP-SEC-Comp-6.2-2 - The Secure Component shall provide following configuration items:

- own network configuration IP addresses (IPv4 or IPv6 or FQDN), hostname, subnet mask, gateway addrsaddress)

- IP addresses / FQDN to all shared cybersecurity services instances (LOG, IAM, PKI, BKP, TIME), support for at least four instances per service for high availability
- maximum access token lifetime
- binding of communication processes to VLANs / interfaces
- days before expiration date to start certificate renewal
- time invalid certificate handling (reject or only issue warning)
- enable automatic session lock
- time period of inactivity of a human user sessionsession
- action after time period of inactivity by human user (lock session or terminate session)

[SPPRAMSS-6672, Generic , no]

, 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. [SPPRAMSS-6886, Generic , no]

, SP-SEC-Comp-6.2-4 - If the Secure Component supports local password-based authentication is used, 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. [SPPRAMSS-6661, Generic , no

Note 3: Common security practices recommend to only change passwords when there is an indication of comprise. Therefore, the maximum password lifetime should be set to infinite (e.g. a long time in the future). [Generic]

, SP-SEC-Comp-6.3-1 - The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in Template in a document accompanying the product. [SPPRAMSS-6894, Generic , no

Note: the product documentation should be available in electronic form in a open file format (defined by an openly published specification as PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG)) [Generic]

, 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. [SPPRAMSS-10305, Generic , no]

, SP-SEC-Comp-6.3-3 - The manufacturer shall make update continuously the Secure Component technical documentation accessible for market surveillance authorities for ten years after the component has been put on the market.

Note: market surveillance authorities as defined in EU 2022/0272 CRA [SPPRAMSS-10307, Generic , no]

, SP-SEC-Comp-6.3-4 - The manufacturer shall create a software bill of materials using the CycloneDX SBOM standard containing 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.. **[**SPPRAMSS-6888, Generic , no **]**

, SP-SEC-Comp-6.3-5 - The software bill of material shall contain at least the data fields defined in **SPPRAMSS-9618 - MinElements_SBOM**. **[**SPPRAMSS-7662, Generic , no **]**

, SP-SEC-Comp-6.4-1 - The manufacturer shall submit an early warning notification to the designated CSIRT and to ENISA of actively exploitable vulnerabilities in Secure Components without undue delay and within 24h of becoming aware of it.

See SPPRAMSS-6857 - Disclosing security-related issues for details of disclosed information including additional potential cross-borders impacts. **[**SPPRAMSS-6881, Generic , no **]**

, SP-SEC-Comp-6.4-2 - The manufacturer shall submit a vulnerability information to the the designated CSIRT and to ENISA of actively exploited vulnerabilities in Secure Components with undue delay and within of 72h of becoming aware of it. **[**SPPRAMSS-10452, Generic , no **]**

, SP-SEC-Comp-6.4-3 - The manufacturer shall submit a final report to the the designated CSIRT and to ENISA of actively exploited vulnerabilities in Secure Components no later than 14 days after a corrcitve or mitigation measure is available.

[SPPRAMSS-10453, Generic , no **]**

, SP-SEC-Comp-6.4-4 - The manufacturer shall submit an early warning notification within 24h to the designated CSIRT and to ENISA of any incident at manufacturer which has impact on the security of the Secure Component including severity, impact, suspicion of unlawful or malicious acts, and cross-border impact.

Note: incident in this context is a successful security breach at the manufacturer **[**SPPRAMSS-6882, Generic , no **]**

, SP-SEC-Comp-6.4-5 - The manufacturer shall submit an incident notification within 72h to the designated CSIRT and to ENISA of any incident at manufacturer which has impact on the security of the Secure Component including general information of the nature of the event, any corrective or mitigating measures. **[**SPPRAMSS-10454, Generic , no **]**

, SP-SEC-Comp-6.4-6 - The manufacturer shall submit an final within 1 month to the designated CSIRT and to ENISA of any incident at manufacturer which has impact on the security of the Secure Component including description, severity, impact, information about malicious actor (when available), security update or other corrective measures. **[**SPPRAMSS-10455, Generic , no **]**

, SP-SEC-Comp-6.4-7 - The manufacturer shall notify without undue delay and after becoming aware, the user of the Secure Component of the incident, including when necessary, corrective measures for mitigating the impact of the incident. **[**SPPRAMSS-6883, Generic , no **]**

, SP-SEC-Comp-6.4-8 - The manufacturer shall provide for mechanisms to securely distribute updates for Secure Components (e.g. using the updated package defined in SPPRAMSS-4030 - Update Package). **[**SPPRAMSS-6892, Generic , no **]**

, SP-SEC-Comp-6.4-9 - The manufacturer shall provide the security patches or updates without undue delay and free of charge for at least five years unless otherwise agreed between manufacturer and business user. **[**SPPRAMSS-6893, Generic , no **]**

, SP-SEC-Comp-6.4-10 - The manufacturer shall ensure that the security patches or updates made available to users during the support periods remains available after it has been released for a minimum of 10 years or the support period, whichever is longer. **[**SPPRAMSS-10450, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-6.4-11 - If a manufacturer ceases operation, the manufacturer shall inform the relevant market authorities and the users of the affected products about this situation. **[**SPPRAMSS-6879, Generic , no **]**

, SP-SEC-Comp-6.4-12 - Update requirements when final version of CRA is available

Change reqs in chapter to give guidance on top of CRA reqs, align with upcoming harmonized standards and final version of CRA **[** Open, SPPRAMSS-7663 **]**

, where appropriate, for at least during the support period. **[**Generic **]**

, SP-SEC-Comp-7.1.1-1 - This section contains the requirements mandatory for COTS network components (switches, routers, gateways, firewalls,...).

Note. Since these products are COTS products, it is not expected that they meet all requirements of Secure Components (chapter 5). **[** Open, SPPRAMSS-7694 **]**

, SP-SEC-Comp-7.1.1-2 - The Network Component shall support IEEE 802.1x EAP TLS network authentication **[**SPPRAMSS-10444, Network , no **]**

, SP-SEC-Comp-7.1.1-3 - The Network Component shall support the RFC 2865 RADIUS protocol for network authenthicationauthentication. **[**SPPRAMSS-10446, Network , no **]**

, SP-SEC-Comp-7.1.1-4 - The Network Component shall support IEEE 802.1q VLAN tagging. **[**SPPRAMSS-10445, Network , no **]**

, SP-SEC-Comp-7.1.1-5 - The Network Component shall support IEEE 802.1q priority code points, also referred as IEEE 801.1p. **[**SPPRAMSS-10448, Network , no **]**

, SP-SEC-Comp-7.1.1-6 - The Network Component shall support ingress policing to enforce bandwidth limitations. This can be fulfilled using Per-Stream Filtering and Policing (PSFP) as of IEEE 802.1Qci. **[**SPPRAMSS-10447, Network , no **]**

, SP-SEC-Comp-7.1.1-7 - The Network Component shall support sending logs and alarms via syslog (RFC 5424), preferable using Syslog over TLS (RFC 5425). **[**SPPRAMSS-2602, Network , no **]**

, SP-SEC-Comp-7.1.1-8 - The Network Component shall support SNMPv3 (RFC 3410). **[**SPPRAMSS-4392, Network , no **]**

, SP-SEC-Comp-7.1.1-9 - The Network Component should support detailed flow information forwarding to analysis system (e.g. RFC 3954 NetFlow, RFC 3176 SFlow) **[**SPPRAMSS-3834, Network , no **]**

, SP-SEC-Comp-7.1.1-10 - The Network Component shall support configuring a separate physical management port. **[**SPPRAMSS-2627, Network , no **]**

, SP-SEC-Comp-7.1.1-11 - The Network Component shall support authentication on all enabled management network interfaces. **[**SPPRAMSS-2524, Network , no **]**

, SP-SEC-Comp-7.1.1-12 - The Network Component shall support integrity and encryption protection for the protocols used for the enabled management network interfaces. **[**SPPRAMSS-6764, Network , no **]**

, SP-SEC-Comp-7.1.1-13 - The Network Component shall support 802.1X on trunk ports **[**Network **]**

, SP-SEC-Comp-7.1.2-1 - If the Network Component supports device access from untrusted networks (e.g. part of a remote access solution), the Network Component shall monitor and control all methods of access. **[**SPPRAMSS-6668, Network , no **]**

, SP-SEC-Comp-7.1.2-2 - If the Network Component supports device access from untrusted networks (e.g. part of a remote access solution), the Network Component shall be capable of deny access requests via untrusted networks unless explicitly approved by an assigned role. **[**SPPRAMSS-6669, Network , no **]**

, 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). **[**SPPRAMSS-2542, Network , no **]**

, 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. **[**SPPRAMSS-3831, Network , no **]**

, SP-SEC-Comp-7.1.3-3 - The Network Component 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) **[**SPPRAMSS-3059, Network , no **]**

, SP-SEC-Comp-7.1.3-4 - The Network Component implementing a firewall shall automatically block connections (fail close) during a failure of the network filter mechanisms. **[**SPPRAMSS-3058, Network , no **]**

, 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. **[**SPPRAMSS-6600, Wireless , no **]**

, SP-SEC-Comp-7.2-1 - If the Secure Component provides a human-machine interface, the Secure Component shall support human user authentication using the central authentication service via SSI-UAS. **[**SPPRAMSS-2293, HMI, yes **]**

, 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 IAM service via SSI-IAM for the corresponding communication session. **[**SPPRAMSS-2292, HMI, yes **]**

, SP-SEC-Comp-7.2-3 - If central security-related components with a human-machine interface (e.g. IAM, software update system) allow critical operations (assign admin role, update security configuration or software), the central high-risk operations, the central security-related Component shall be capable to enforce the dual control principle. **[**SPPRAMSS-2972, HMI, no

Note. Examples for high-risk operations are: assign admin role, update security configuration or software. **[**HMI **]**

, **SP-SEC-Comp-7.2-4 -** If the Secure Component provides a human-machine interfaces, the Secure Component shall lock or terminate sessions after a time period of inactivity depending on configuration. **[**SPPRAMSS-2296, HMI, yes **]**

, **SP-SEC-Comp-7.2-5 -** If the Secure Component provides a human-machine interfaces, the Secure Component shall enable the human user to lock or terminate sessions manually. **[**SPPRAMSS-7708, HMI, yes **]**

, **SP-SEC-Comp-7.2-6 -** If the Secure Component provides a human-machine interfaces, the Secure Component shall unlock the locked human-user sessions only after re-authentication of the human user.

See also SPPRAMSS-6670 for Note: See also SP-SEC-Comp-7.2-7 for supervisor override in case of HMI controlling essential services. **[**SPPRAMSS-6693, HMI, yes **]**

, **SP-SEC-Comp-7.2-7 -** If a 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. **[**SPPRAMSS-6670, HMI, yes **]**

, **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. **[**HMI **]**

, **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) **[**HMI **]**

, **SP-SEC-Comp-7.2-10 -** If the Secure Component provides a human-machine interface, the human-machine interface shall be designed considering human-factors.

Note: this ensures that security functions can be operated easily and without faults by human users. The recommended standard for human-factors is **[EN ISO 14915]** **[**[Component Type] **]**

, **SP-SEC-Comp-7.3-1 -** This section is for Secure Components that use local password-based authentication and local user management for their interfaces and do . e.g. it does not integrate into an user authentication service (SCS-UAS) password-based authentication. **[** Open, SPPRAMSS-6654 **]**

, **SP-SEC-Comp-7.3-2 -** If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports local password-based authentication and local user management, then Secure Component shall enforce configurable password strength (minimum length, variety of character types). **[**SPPRAMSS-6655, Generic , no **]**

, **SP-SEC-Comp-7.3-3 -** If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports 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. **[**SPPRAMSS-6658, Generic , no **]**

, **SP-SEC-Comp-7.3-4 -** If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports 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. **[**SPPRAMSS-6656, Generic , no **]**

, **SP-SEC-Comp-7.3-5 -** If the Secure Component uses password authentication and does not use the interface

SSI-UAS for password-based authenticationsupports local password-based authentication and local user management, then the Secure Component shall provide the capability to prompt the human user to change their password upon a configurable time prior expiration. **[**SPPRAMSS-6657, Generic , no **]**

, SP-SEC-Comp-7.3-6 - If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports 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). **[**SPPRAMSS-3885, Generic , no **]**

, SP-SEC-Comp-7.3-7 - If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports 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. **[**SPPRAMSS-6664, Generic , no **]**

, SP-SEC-Comp-7.3-8 - If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-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

[SPPRAMSS-6663, Generic , no **]**

, SP-SEC-Comp-7.3-9 - If the Secure Component uses password authentication and does not use the interface SSI-UAS for password-based authenticationsupports 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 invalid user" or "invalide invalid password", "password length insufficient". **[**SPPRAMSS-2966, Generic , no **]**

, 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. **[**SPPRAMSS-6665, Generic , no **]**

, SP-SEC-Comp-7.4-2 - If symmetric symmetric key-based authentication is used due to interoperability requirements by TSI, the Secure Component shall ensure that algorithms and keys used for the protect the symmetric key authentication conform to internationally recognized and proved security practices and recommendations.

Note-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 symmmetric symmetric keys ensuring confidentiality. This can be done using PKI / asymmetric cryptography or a out-of-band transmission ensuring confidentiality. [SPPRAMSS-6666, Generic , no

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) **[**Generic **]**

Requirements for additional communication beyond TSI/SP standardized interfaces (e.g. SCI, SMI, SDI, SSI, UNISIG subset-146,148, 137). To-Do: give clear references to standardized interfaces

Examples of additional communication interfaces: Web Server, SSH, FTPS,...

In general, all maintenance and diagnostic activities should be conducted using existing interfaces (e.g. SDI, SMI,...).

Direct access to the operating system is not advisable and should be avoided.

, SP-SEC-Comp-7.5-1 - Rework section

Rework section with generic requirements for communication interfaces (align with rest of doc and with IEC 62443-4-2).

Move whole section to Secure Comm Spec **[** Open, SPPRAMSS-6772 **]**

,

The following general risks remain after applying the three System Pillar Cybersecurity technical requirements specifications ([SP-SEC-CompSpec], [SP-SEC-CompSpec], and [SP-SEC-ServSpec])

, SP-SEC-Comp-78.5.1-1 - The Secure Component shall provide a unique identifier for each communicating process.

Note: examples of unique identifiers are FQDN, UUID, IP-address combined with a local unique identifier (e.g. process name, process idSecure Components and Network Components are complex products composed of various hardware (chipsets, CPU,...) . **[**SPPRAMSS-2482, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-7.5.1-2 - The Secure Component shall authenticate each communication partner.

Note: This ensures mutual authentication between communication partners. **[**SPPRAMSS-4683, [Component Type], [Requirements supports essential function] **]**

Note: this section has similar requirements as the Secure Communication Specification, but are for other interfaces and communication protocols.

and software (Open Source SW components, 3rd party SW components,...). Vulnerabilities are found and mostly documented in vulnerability databases. In recent years, these database documented thousands of new vulnerabilities.

, SP-SEC-Comp-78.5.1-2 -1 - The Secure Component shall protect the integrity of data in transit using state of the art cryptographic methods.

To-Do: define state of the art **[**SPPRAMSS-2478, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-7.5.2-2 - If the Secure Component has a safety certification, the Secure Component's shall be capable to update the cryptographic protocols and parameters without invalidating its safety certification. **[**SPPRAMSS-2480, [Component Type], [Requirements supports essential function] **]**

risk caused by vulnerabilities in Secure Components and Network Components are reduced by the Defense-in-depth design of the System Pillar technical specifications. However, as time passes, more vulnerabilities are detected and can lead to an exploitable vulnerability.

, SP-SEC-Comp-78.5.21-3 - The Secure Component shall use cryptographic integrity protection. **[**SPPRAMSS-2483, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-7.5.2-4 - The Secure Component shall support periodic re-authentication during an active session for the TLS connection. **[**SPPRAMSS-2485, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-7.5.2-5 - The Secure Component shall support separate re-authentication per TLS connection. **[**SPPRAMSS-2484, [Component Type], [Requirements supports essential function] **]**

Mitigation: Vulnerability Management (as defined in IEC 62443-4-1 DM1-DM6) and installation of security updates

(see SP-SEC-PrgmReq Ch 8.1-21 - Updating Secure Components)

, SP-SEC-Comp-78.5.2-61 - The Secure Component shall provide the capability to use integrity-only ciphers for connections not requiring confidentiality. **[**SPPRAMSS-2487, [Component Type], [Requirements supports essential function] **]**

Secure Components and Network Components can be compromised by attackers when privileged accounts, especially from the implementations of SCS-IAM, SCS-UAS, SCS-BKP and software update and configuration systems, have been compromised.

, SP-SEC-Comp-78.5.2-72 - The Secure Component shall provide the capability to use encryption ciphers for connections requiring confidentiality. **[**SPPRAMSS-6887, [Component Type], [Requirements supports essential function] **]**

, SP-SEC-Comp-7.5.2-8 - The Secure Component shall provide the capability to activate and deactivate integrity-only ciphers in a secure manner. **[**SPPRAMSS-2486, [Component Type], [Requirements supports essential function] **]**

Attackers can use these accounts to add themselves as legitimate users, even with elevated privileges, and access components which implement access control. Attackers can also install previous configurations or firmware with exploitable vulnerabilities (downgrade attack) or when the software signing keys are also compromised, install malware-infected software or configurations disabling security features.

, SP-SEC-Comp-78.5.2-9 - The Secure Component shall prevent connected users (i.e., humans, software processes, or hardware devices) from using the Secure Component's functionalities to generate DoS attacks. **[**SPPRAMSS-3076, [Component Type], [Requirements supports essential function] **]**

3 - Compromise of privileged accounts can be caused by social attacks (e.g. phising, black mailing, quid pro quo, water-holing,...).

, SP-SEC-Comp-8.2-1 - Add Tolarable risk, risk acceptance

Add Tolarable risk, risk acceptance **[** Open, SPPRAMSS-10442 **]**

, **4 -** Mitigation: Training of security operators against account compromise and awareness of social attack threats (see SP-SEC-Comp-8-2 - Add Security related application conditions (SecRACs)

Add Security related application conditions (SecRACs) **[** Open, SPPRAMSS-10441 **]**

Requirements mapping from EU cybersecurity legislation (NIS, Cybersecurity Act, Cyber Resiliency Act, IEC 62443-4-2)

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

, Prgm Ch 5.10 - Personell awareness training)

, SP-SEC-Comp-98.1.13-1 - 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 requirement for password life-time restrictions. Requirement not needed. **[**SPPRAMSS-7711, [Component Type], [Requirements supports essential function] **]**

Secure Component and Network Components can be compromised by introducing vulnerabilities in the supply chain. This can lead to undetected and undocumented exploitable vulnerabilities.

, SP-SEC-Comp-98.1.13-2 - 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.

Issue: check if reference to this can be given **[**SPPRAMSS-6662, [Component Type], [Requirements supports essential function] **]**

, Several cases of supply chain attacks of hardware chipsets, open source software and 3rd party software has been recorded over the last years.

, SP-SEC-Comp-98.1.13-3 - NOT IMPLEMENTED: EDR/NDR/HDR 2.13 RE1: monitoring of physical factory diagnostic and test interfaces are disabled. Monitoring these interfaces 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). **[**SPPRAMSS-6696, [Component Type], [Requirements supports essential function] **]**

Supply chain attacks are hard to be detected and hard to be mitigated. They can only be detected by change reviews (suitable mainly for open source software) or by anomaly detection during operation.

, SP-SEC-Comp-98.1.13-4 - 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 an allowlist for software processes to protect against the execution unauthorised software. See ~~SPPRAMSS-3425~~ - The Secure Component shall ensure the runtime-integrity of executables. **[**SPPRAMSS-6740, [Component Type], [Requirements supports essential function] **]**

Mitigation: Review of relevant open source components (this can be practicable only be done on an international level, spanning industry sectors and national boundaries). This is due to the required effort and benefit structure (high effort not feasible for an individual company, once detected the benefit is across industry sectors and national boundaries). Therefore, a funding to conduct change analysis on relevant open source components in necessary at least at a European level.

, SP-SEC-Comp-98.1.13-5 - 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 connect a log/audit storage via a network tap. **[**SPPRAMSS-6742, [Component Type], [Requirements supports essential function] **]**Mitigation: Anomaly detection systems (e.g. in NIDS) should be employed in environments of installed Secure Components to detect unexpected behaviour and communication attempts.

, SP-SEC-Comp-98.4-1.1 -6 - DO NOT comment to th table below (this is an automatically created table and will be replaced regularly until baseline creation). Comment on this line or on corresponding requirement for linking errors. **[** Open, SPPRAMSS-6635 **]**

, SP-SEC-Comp-9.1.1-7 - No additional application conditions have been identified beyond the requirements specified in the SP Cybersecurity requirements documents.

old ID	Title	Linked Work Items

old ID	Title	Linked Work Items
IEC 62443-4-2 CCSC 1	Support for essential functions	implements: SPPRAMSS-2636 - The Secure Component shall limit use of system resources by security functions t... implements: SPPRAMSS-3781 - After a Denial of Service (DoS) event (e.g. saturation / high load of the networ... implements: SPPRAMSS-6670 - If a Secure Component implements a human-machine interface which is needed to co...
IEC 62443-4-2 CCSC 2	Compensating countermeasures	implements: SPPRAMSS-9637 - If a requirement of this specification is not implemented, the component documen... implements: SPPRAMSS-9638 - If a requirement of this specification is not implemented, the component documen...
IEC 62443-4-2 CCSC 3	Least privilege	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the... implements: SPPRAMSS-2311 - The Secure Component shall enforce access based on retrieved permissions for all... implements: SPPRAMSS-9989 - The Secure Component shall validate and enforce the extended key usage according...
IEC 62443-4-2 CCSC 4	Software development process	implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
IEC 62443-4-2 CR 1.01	Human user identification and authentication	implements: SPPRAMSS-4683 - The Secure Component shall authenticate each communication partner. implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the...
IEC 62443-4-2 CR 1.01 RE 1	Unique identification and authentication	implements: SPPRAMSS-4683 - The Secure Component shall authenticate each communication partner.
IEC 62443-4-2 CR 1.01 RE 2	Multifactor authentication for all interfaces	implements: SPPRAMSS-4675 - The SSI-UAS shall support multi-factor authentication of human users. implements: SPPRAMSS-6574 - The SSI-UAS shall support authentication with username/password with at least on... implements: SPPRAMSS-6575 - The SSI-UAS shall support authentication with X.509 client certificates complyin... implements: SPPRAMSS-6576 - The SSI-UAS should support passwordless authentication with at least one additio...
IEC 62443-4-2 CR 1.02	Software process and device identification and authentication	implements: SPPRAMSS-2482 - The Secure Component shall provide a unique identifier for each communicating pr... implements: SPPRAMSS-3999 - The Secure Component shall authenticate each communication partner by validating...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 1.02 RE 1	Unique identification and authentication	implements: SPPRAMSS-3999 - The Secure Component shall authenticate each communication partner by validating... implements: SPPRAMSS-2967 - The Secure Component shall be capable of utilizing a unique X.509 v3 certificate...
IEC 62443-4-2 CR 1.03	Account management	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the...
IEC 62443-4-2 CR 1.04	Identifier management	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the... implements: SPPRAMSS-4975 - The SSI-IAM server shall have the possibility to retrieve identities from an ide...
IEC 62443-4-2 CR 1.05	Authenticator management	implements: SPPRAMSS-2941 - The Secure Component shall protect the integrity and confidentiality of critical... implements: SPPRAMSS-2335 - The Secure Component shall automatically request the renewal of its certificates... implements: SPPRAMSS-4961 - The Secure Component shall request the Operator Device Certificate (ODC) via the... implements: SPPRAMSS-4962 - The Secure Component shall request all other operator certificates (ONCC, OSCC,... implements: SPPRAMSS-4967 - The Secure Component shall have the capability to install trusted certificates i...
IEC 62443-4-2 CR 1.05 RE 1	Hardware security for authenticators	implements: SPPRAMSS-3105 - The Secure Component shall use the Secure Boot functions defined by the used chi... implements: SPPRAMSS-3099 - The Secure Component shall protect the integrity of roots of trust (root certifi... implements: SPPRAMSS-2941 - The Secure Component shall protect the integrity and confidentiality of critical...
IEC 62443-4-2 CR 1.07	Strength of password-based authentication	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the... implements: SPPRAMSS-6655 - If the Secure Component uses password authentication and does not use the interf... implements: SPPRAMSS-6661 - If password based authentication is used, the Secure Component shall provide fol...
IEC 62443-4-2 CR 1.07 RE 1	Password generation and lifetime restrictions for human users	implements: SPPRAMSS-6656 - If the Secure Component uses password authentication and does not use the interf... implements: SPPRAMSS-6658 - If the Secure Component uses password authentication and does not use the interf...
IEC 62443-4-2 CR 1.07 RE 2	Password lifetime restrictions for all users (human, software process, or device...	implements: SPPRAMSS-7711 - NOT IMPLEMENTED: CR 1.7 RE 2: Password life-time restrictions for all users (hum...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 1.08	Public key infrastructure certificates	implements: SPPRAMSS-2324 - The Secure Component shall implement the interface to request certificates. implements: SPPRAMSS-2322 - The Secure Component shall implement the interfaces to renew a certificate.
IEC 62443-4-2 CR 1.09	Strength of public key-based authentication	implements: SPPRAMSS-2430 - The Secure Component shall check if the certificate signature is valid. implements: SPPRAMSS-2431 - The Secure Component shall check if the certificate is not revoked using CRLs. implements: SPPRAMSS-2432 - The Secure Component shall validate the certificate's trust chain up to a truste... implements: SPPRAMSS-6660 - The Secure Component shall map the authenticated identity of a certificate to a...
IEC 62443-4-2 CR 1.09 RE 1	Hardware security for public key-based authentication	implements: SPPRAMSS-2941 - The Secure Component shall protect the integrity and confidentiality of critical...
IEC 62443-4-2 CR 1.10	Authenticator feedback	implements: SPPRAMSS-2966 - If the Secure Component uses password authentication and does not use the interf...
IEC 62443-4-2 CR 1.11	Unsuccessful login attempts	implements: SPPRAMSS-6663 - If the Secure Component uses password authentication and does not use the interf... implements: SPPRAMSS-3885 - If the Secure Component uses password authentication and does not use the interf... implements: SPPRAMSS-6664 - If the Secure Component uses password authentication and does not use the interf... implements: SPPRAMSS-6661 - If password based authentication is used, the Secure Component shall provide fol...
IEC 62443-4-2 CR 1.12	System use notification	implements: SPPRAMSS-6662 - NOT IMPLEMENTED: CR 1.12. System use notification is required by US law for lega...
IEC 62443-4-2 CR 1.14	Strength of symmetric key-based authentication	implements: SPPRAMSS-2941 - The Secure Component shall protect the integrity and confidentiality of critical... implements: SPPRAMSS-6666 - If symmetric key-based authentication is used, the Secure Component shall ensure... implements: SPPRAMSS-6665 - If symmetric key-based authentication is used, the Secure Component shall establ...
IEC 62443-4-2 CR 1.14 RE 1	Hardware security for symmetric key-based authentication	implements: SPPRAMSS-2941 - The Secure Component shall protect the integrity and confidentiality of critical...
IEC 62443-4-2 CR 2.01	Authorization enforcement	implements: SPPRAMSS-2311 - The Secure Component shall enforce access based on retrieved permissions for all...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 2.01 RE 1	Authorization enforcement for all users (human, software process, and devices)	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the... implements: SPPRAMSS-2311 - The Secure Component shall enforce access based on retrieved permissions for all...
IEC 62443-4-2 CR 2.01 RE 2	Permission mapping to roles	implements: SPPRAMSS-2310 - The Secure Component shall use the interface [SSI-IAM] in order to retrieve the...
IEC 62443-4-2 CR 2.01 RE 3	Supervisor override	implements: SPPRAMSS-6670 - If a Secure Component implements a human-machine interface which is needed to co...
IEC 62443-4-2 CR 2.01 RE 4	Dual approval	implements: SPPRAMSS-2972 - If central components with a human-machine interface (e.g. IAM, software update...
IEC 62443-4-2 CR 2.02	Wireless use control	implements: SPPRAMSS-6600 - If a Network Component supports wireless access management (e.g. WLAN access poi...
IEC 62443-4-2 CR 2.05	Session lock	implements: SPPRAMSS-2296 - If the Secure Component provides a human-machine interfaces, the Secure Componen... implements: SPPRAMSS-6693 - If the Secure Component provides a human-machine interfaces, the Secure Componen...
IEC 62443-4-2 CR 2.06	Remote session termination	implements: SPPRAMSS-2296 - If the Secure Component provides a human-machine interfaces, the Secure Componen...
IEC 62443-4-2 CR 2.07	Concurrent session control	implements: SPPRAMSS-2630 - The Secure Component shall provide the capability to only allow a configurable m...
IEC 62443-4-2 CR 2.08	Auditable events	implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events: implements: SPPRAMSS-2588 - The Secure Component shall send log messages complying to the log message format...
IEC 62443-4-2 CR 2.09	Audit storage capacity	implements: SPPRAMSS-2596 - If the storage capacity is exceeded, the Secure Component shall overwrite the ol... implements: SPPRAMSS-2598 - The Secure Component shall be able to store untransferred log data for eight hou...
IEC 62443-4-2 CR 2.09 RE 1	Warn when audit record storage capacity threshold reached	implements: SPPRAMSS-3070 - If the storage capacity has reached a defined threshold, the Secure Component sh...
IEC 62443-4-2 CR 2.10	Response to audit processing failures	implements: SPPRAMSS-4439 - If the Secure Component starts overwriting not transferred log data, it shall ge... implements: SPPRAMSS-2596 - If the storage capacity is exceeded, the Secure Component shall overwrite the ol... implements: SPPRAMSS-3070 - If the storage capacity has reached a defined threshold, the Secure Component sh...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 2.11	Timestamps	implements: SPPRAMSS-2580 - The Secure Component shall send the logging events via SSI-LOG . implements: SPPRAMSS-4819 - The Log originator shall set the timestamp of the syslog header to the current t...
IEC 62443-4-2 CR 2.11 RE 1	Time synchronization	implements: SPPRAMSS-2301 - The Secure Component shall synchronize the component time using [SSI-STS] secure...
IEC 62443-4-2 CR 2.11 RE 2	Protection of time source integrity	implements: SPPRAMSS-2301 - The Secure Component shall synchronize the component time using [SSI-STS] secure... implements: SPPRAMSS-3701 - The SSI-STS client shall use NTS as specified in RFC 8915.
IEC 62443-4-2 CR 2.12	Non-repudiation	implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events:
IEC 62443-4-2 CR 2.12 RE 1	Non-repudiation for all users	implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events: implements: SPPRAMSS-2588 - The Secure Component shall send log messages complying to the log message format...
IEC 62443-4-2 CR 3.01	Communication integrity	implements: SPPRAMSS-6675 - The Secure Component shall implement the interfaces defined in .
IEC 62443-4-2 CR 3.01 RE 1	Communication authentication	implements: SPPRAMSS-6676 - If the Secure Component uses the standard communication protocols defined in , t... implements: SPPRAMSS-6675 - The Secure Component shall implement the interfaces defined in .
IEC 62443-4-2 CR 3.03	Security functionality verification	
IEC 62443-4-2 CR 3.03 RE 1	Security functionality verification during normal operation	implements: SPPRAMSS-10142 - The Secure Component
IEC 62443-4-2 CR 3.04	Software and information integrity	implements: SPPRAMSS-3429 - If a secure boot verification fails, the Secure Component shall provide a visibl... implements: SPPRAMSS-3105 - The Secure Component shall use the Secure Boot functions defined by the used chi... implements: SPPRAMSS-2471 - The Secure Component shall verify the integrity and authenticity of configuratio... implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events:

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 3.04 RE 1	Authenticity of software and information	implements: SPPRAMSS-3429 - If a secure boot verification fails, the Secure Component shall provide a visibl... implements: SPPRAMSS-3105 - The Secure Component shall use the Secure Boot functions defined by the used chi... implements: SPPRAMSS-2471 - The Secure Component shall verify the integrity and authenticity of configuratio... implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events:
IEC 62443-4-2 CR 3.04 RE 2	Automated notification of integrity violations	implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events:
IEC 62443-4-2 CR 3.05	Input validation	implements: SPPRAMSS-3023 - The Secure Component shall validate the syntax, length and content of any input...
IEC 62443-4-2 CR 3.06	Deterministic output	implements: SPPRAMSS-4998 - The supplier shall document the predetermined state for Secure Component with ph... implements: SPPRAMSS-3022 - If the Secure Component has physical I/O controlling an automation process, the...
IEC 62443-4-2 CR 3.07	Error handling	implements: SPPRAMSS-2580 - The Secure Component shall send the logging events via SSI-LOG . implements: SPPRAMSS-4404 - The communication partners using the SSI-LOG (Log Originator, Log Relay, Log Col...
IEC 62443-4-2 CR 3.08	Session integrity	implements: SPPRAMSS-6055 - The SSI-UAS shall implement single sign-on (SSO) based on OpenID Connect 1.0 (OI... implements: SPPRAMSS-6676 - If the Secure Component uses the standard communication protocols defined in , t... implements: SPPRAMSS-6675 - The Secure Component shall implement the interfaces defined in . implements: SPPRAMSS-5803 - The SSI-IAM shall accept SCIM 2.0 requests over REST over HTTPS according to RFC... implements: SPPRAMSS-4070 - The SSI-PKI client shall provide the capability to request and rekey certificate... implements: SPPRAMSS-4404 - The communication partners using the SSI-LOG (Log Originator, Log Relay, Log Col...
IEC 62443-4-2 CR 3.09	Protection of audit information	implements: SPPRAMSS-2488 - For retrieval of log data, the Secure Component shall protect the integrity of l... implements: SPPRAMSS-2580 - The Secure Component shall send the logging events via SSI-LOG .
IEC 62443-4-2 CR 3.09 RE 1	Audit records on write-once media	implements: SPPRAMSS-6742 - NOT IMPLEMENTED: CR 3.9 RE 1: using hardware-enforced write-once media to store...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 4.1	Information confidentiality	implements: SPPRAMSS-3013 - If read access authorisation to persistent data is required, the Secure Componen... implements: SPPRAMSS-6676 - If the Secure Component uses the standard communication protocols defined in , t... implements: SPPRAMSS-6675 - The Secure Component shall implement the interfaces defined in .
IEC 62443-4-2 CR 4.2	Information persistence	implements: SPPRAMSS-6748 - The Secure Component shall provide the maintenance method Security:FactoryReset(...
IEC 62443-4-2 CR 4.2 RE 1	Erase of shared memory resources	implements: SPPRAMSS-9632 - The Secure Component shall use for the implementation of security functionality...
IEC 62443-4-2 CR 4.2 RE 2	Erase verification	implements: SPPRAMSS-6748 - The Secure Component shall provide the maintenance method Security:FactoryReset(... implements: SPPRAMSS-9632 - The Secure Component shall use for the implementation of security functionality...
IEC 62443-4-2 CR 4.3	Use of cryptography	implements: SPPRAMSS-2471 - The Secure Component shall verify the integrity and authenticity of configuratio...
IEC 62443-4-2 CR 5.1	Network segmentation	implements: SPPRAMSS-2315 - The Secure Component shall support to authenticate to the network using the SSI-... implements: SPPRAMSS-7528 - The Secure Component shall be capable to separate at least maintenance (e.g. SMI... implements: SPPRAMSS-7526 - The Secure Component shall be capable to bind each communicating process to conf...
IEC 62443-4-2 CR 6.1	Audit log accessibility	implements: SPPRAMSS-4203 - The Secure Component shall provide the mainteance method Security:GetSecurityLog...
IEC 62443-4-2 CR 6.1 RE 1	Programmatic access to audit logs	implements: SPPRAMSS-4203 - The Secure Component shall provide the mainteance method Security:GetSecurityLog...
IEC 62443-4-2 CR 6.2	Continuous monitoring	implements: SPPRAMSS-2580 - The Secure Component shall send the logging events via SSI-LOG . implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events: implements: SPPRAMSS-3425 - The Secure Component shall use a process allowlist to protect against execution...
IEC 62443-4-2 CR 7.1	Denial of service protection	implements: SPPRAMSS-3821 - The host-based firewall shall deny by default all inbound and outbound connectio... implements: SPPRAMSS-9633 - The Secure Component shall limit use of system resources by security functions t... implements: SPPRAMSS-3781 - After a Denial of Service (DoS) event (e.g. saturation / high load of the networ...

old ID	Title	Linked Work Items
IEC 62443-4-2 CR 7.1 RE 1	Manage communication loads	implements: SPPRAMSS-2630 - The Secure Component shall provide the capability to only allow a configurable m... implements: SPPRAMSS-3781 - After a Denial of Service (DoS) event (e.g. saturation / high load of the networ...
IEC 62443-4-2 CR 7.2	Resource management	implements: SPPRAMSS-2636 - The Secure Component shall limit use of system resources by security functions t...
IEC 62443-4-2 CR 7.3	Control system backup	implements: SPPRAMSS-3078 - If operational data is not part of the configuration data from (interface, the S... implements: SPPRAMSS-6750 - If the Secure Component backups operational data , the Secure Component shall be...
IEC 62443-4-2 CR 7.3 RE 1	Backup integrity verification	implements: SPPRAMSS-6750 - If the Secure Component backups operational data , the Secure Component shall be... implements: SPPRAMSS-6749 - If the Secure Component backups operational data, the Secure Component shall be...
IEC 62443-4-2 CR 7.4	Control system recovery and reconstitution	implements: SPPRAMSS-2497 - The Secure Component shall support the update of software and configuration via... implements: SPPRAMSS-6749 - If the Secure Component backups operational data, the Secure Component shall be...
IEC 62443-4-2 CR 7.6	Network and security configuration settings	implements: SPPRAMSS-3088 - The Secure Component shall provide the maintenance method Security:GetNetworkCon...
IEC 62443-4-2 CR 7.6 RE 1	Machine-readable reporting of current security settings	implements: SPPRAMSS-3088 - The Secure Component shall provide the maintenance method Security:GetNetworkCon...
IEC 62443-4-2 CR 7.7	Least functionality	implements: SPPRAMSS-2626 - If unnecessary drivers and software components cannot be removed, the supplier s... implements: SPPRAMSS-3779 - The Secure Component shall implement the hardening measures according to the rel...
IEC 62443-4-2 CR 7.8	Control system component inventory	implements: SPPRAMSS-4960 - The Secure Component shall be equipped with a Manufacturer Device Certificate (M... implements: SPPRAMSS-10138 - The Secure Component shall provide the maintenance method Security:GetInstalledC... implements: SPPRAMSS-10141 - The Secure Component shall provide the maintenance method Security:GetComponentC...
IEC 62443-4-2 EDR/HDR/NDR 2.13	Use of physical diagnostic and test interfaces	implements: SPPRAMSS-6695 - If physical diagnostic and test interfaces are accessible without opening the pr...
IEC 62443-4-2 EDR/HDR/NDR 2.13 RE 1	Active monitoring	implements: SPPRAMSS-6696 - NOT IMPLEMENTED: EDR/NDR/HDR 2.13 RE1: monitoring of physical factory diagnostic...

old ID	Title	Linked Work Items
IEC 62443-4-2 EDR/HDR/NDR 3.10	Support for updates	implements: SPPRAMSS-2497 - The Secure Component shall support the update of software and configuration via...
IEC 62443-4-2 EDR/HDR/NDR 3.10 RE 1	Update authenticity and integrity	implements: SPPRAMSS-2982 - The Secure Component shall verify the signature of the update packages using the...
IEC 62443-4-2 EDR/HDR/NDR 3.11	Physical tamper resistance and detection	implements: SPPRAMSS-2994 - The supplier shall provide a security seal on the Secure Component. implements: SPPRAMSS-3111 - When powered the Secure Component shall provide a tamper detection mechanism whi...
IEC 62443-4-2 EDR/HDR/NDR 3.11 RE 1	Notification of a tampering attempt	implements: SPPRAMSS-3110 - If tampering is detected, the Secure Component shall provide notification of the...
IEC 62443-4-2 EDR/HDR/NDR 3.12	Provisioning product supplier roots of trust	implements: SPPRAMSS-2308 - Before commissioning the Secure Component shall retrieve and store its Manufactu...
IEC 62443-4-2 EDR/HDR/NDR 3.13	Provisioning asset owner roots of trust	implements: SPPRAMSS-3729 - The Secure Component shall continue with the next boot stage only if the integri... implements: SPPRAMSS-2473 - If an integrity check of a secure boot stage fails during secure boot, the Secur... implements: SPPRAMSS-3105 - The Secure Component shall use the Secure Boot functions defined by the used chi... implements: SPPRAMSS-4961 - The Secure Component shall request the Operator Device Certificate (ODC) via the...
IEC 62443-4-2 EDR/HDR/NDR 3.14	Integrity of the boot process	implements: SPPRAMSS-4911 - The Secure Component shall verify all secure boot stages from start of the hardw... implements: SPPRAMSS-3105 - The Secure Component shall use the Secure Boot functions defined by the used chi...
IEC 62443-4-2 EDR/HDR/NDR 3.14 RE 1	Authenticity of the boot process	implements: SPPRAMSS-6577 - The Secure Component shall use the certificate chain up to the Manufacturer Root...
IEC 62443-4-2 HDR 3.02 RE 1	Report version of code protection	implements: SPPRAMSS-6740 - NOT IMPLEMENTED: HDR 3.2 RE 1: reporting the version of software and files for c...
IEC 62443-4-2 NDR 1.06	Wireless access management	implements: SPPRAMSS-6600 - If a Network Component supports wireless access management (e.g. WLAN access poi...
IEC 62443-4-2 NDR 1.06 RE 1	Unique identification and authentication	implements: SPPRAMSS-6600 - If a Network Component supports wireless access management (e.g. WLAN access poi...
IEC 62443-4-2 NDR 1.13	Access via untrusted networks	implements: SPPRAMSS-6668 - If the Network Component supports device access from untrusted networks (e.g. pa...

old ID	Title	Linked Work Items
IEC 62443-4-2 NDR 1.13 RE 1	Explicit access request approval	implements: SPPRAMSS-6669 - If the Network Component supports device access from untrusted networks (e.g. pa...
IEC 62443-4-2 NDR 5.2	Zone boundary protection	implements: SPPRAMSS-2542 - The Network Component implementing a firewall shall be capable of deny-all and a... implements: ~~SPPRAMSS-3061~~ - The Network Component implementing a firewall shall send information regarding b...
IEC 62443-4-2 NDR 5.2 RE 1	Deny by default, permit by exception	implements: SPPRAMSS-2542 - The Network Component implementing a firewall shall be capable of deny-all and a...
IEC 62443-4-2 NDR 5.2 RE 2	Island mode	implements: SPPRAMSS-3059 - The Network Component implementing a firewall shall be capable of enabling an is...
IEC 62443-4-2 NDR 5.2 RE 3	Fail close	implements: SPPRAMSS-3058 - The Network Component implementing a firewall shall automatically block connecti...
IEC 62443-4-2 NDR 5.3	General purpose person-to-person communication restrictions	implements: SPPRAMSS-2542 - The Network Component implementing a firewall shall be capable of deny-all and a... implements: SPPRAMSS-3831 - The Network Component implementing a firewall shall be capable of packet filteri...
IEC 62443-4-2 SAR/EDR/HDR/NDR 2.04	Mobile code	implements: SPPRAMSS-3084 - The Secure Component shall prevent the execution of mobile code unless its integ...
IEC 62443-4-2 SAR/EDR/HDR/NDR 2.04 RE 1	Mobile code integrity check	implements: SPPRAMSS-2984 - The Secure Component shall reject update packages without a valid signature. implements: SPPRAMSS-2982 - The Secure Component shall verify the signature of the update packages using the... implements: SPPRAMSS-3084 - The Secure Component shall prevent the execution of mobile code unless its integ...
IEC 62443-4-2 SAR/EDR/HDR/NDR 3.02	Protection from malicious code	implements: SPPRAMSS-2982 - The Secure Component shall verify the signature of the update packages using the... implements: SPPRAMSS-3425 - The Secure Component shall use a process allowlist to protect against execution...

97 items found

(type:srq AND (document.title:62443\-4\-2)) AND project.id:SPPRAMS

[Open, SPPRAMSS-7487]

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

This section will be filled in the next version of this document.

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

This section will be filled in the next version of this document.

, SP-SEC-Comp-9.4-1 - Table containing tracing to EU-CRA (EU 2022/0272 - COD) req no, title and corresponding req or chapter link

Note: this table will be updated with the final version of the EU-CRA in the next version of this specification.

EU CRA	Requirment	Linked Work Items
EU-CRA 06-01	(1) they meet the essential requirements set out in Part I of Annex I, provided...	implements: SPPRAMSS-5544 - Annex I - Part I - Essential Cybersecurity requirements
EU-CRA 06-02	(2) the processes put in place by the manufacturer comply with the essential req...	implements: SPPRAMSS-5336 - Annex I-2 Vulnerability Handling Requirements
EU-CRA 13-01	1. When placing a product with digital elements on the market, manufacturers sha...	implements: SPPRAMSS-5544 - 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, m...	implements: SPPRAMSS-6828 - SR-2 Threat model implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-03	The cybersecurity risk assessment shall be documented and updated as appropriate...	implements: SPPRAMSS-6828 - SR-2 Threat model implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-04	When placing a product with digital elements on the market, the manufacturer sha...	implements: SPPRAMSS-5318 - Article 31- Technical documentation implements: SPPRAMSS-5466 - Risk assessment implements: SPPRAMSS-10269 - Security risks implements: SPPRAMSS-10286 - Adressed threats
EU-CRA 13-05	For the purpose of complying with paragraph 1, manufacturers shall exercise due...	implements: SPPRAMSS-6807 - SM-10: Custom developed components from third-party suppliers implements: SPPRAMSS-6811 - SM-9: Security requirements for externally provided components implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-06	Manufacturers shall, upon identifying a vulnerability in a component, including...	implements: SPPRAMSS-6828 - SR-2 Threat model implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-07	The manufacturers shall systematically document, in a manner that is proportiona...	implements: SPPRAMSS-10287 - Security properties implements: SPPRAMSS-10269 - Security risks implements: SPPRAMSS-10253 - Vulnerability reporting

EU CRA	Requirment	Linked Work Items
EU-CRA 13-08-01	Manufacturers shall ensure, when placing a product with digital elements on the...	implements: SPPRAMSS-6857 - DM-5: Disclosing security-related issues implements: SPPRAMSS-6859 - DM-4: Addressing security-related issues implements: SPPRAMSS-6844 - DM-3: Assessing security-related issues implements: SPPRAMSS-5344 - Manufacturers of the products with digital elements shall put in place and enfor... implements: SPPRAMSS-5362 - Annex III - Important Products with Digital Elements implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-08-02	Manufacturers shall determine the support period so that it reflects the length...	implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-08-03	Without prejudice to the second subparagraph, the support period shall be at lea...	implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-08-05	Manufacturers shall include the information that was taken into account to deter...	implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-08-06	Manufacturers shall have appropriate policies and procedures, including coordina...	implements: SPPRAMSS-10249 - Vulnerability reporting policy implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-09	Manufacturers shall ensure that each security update, as referred to in Part II,...	implements: SPPRAMSS-10307 - The manufacturer shall make the Secure Component technical documentation accessi...
EU-CRA 13-12	Before placing a product with digital elements on the market, manufacturers shal...	implements: SPPRAMSS-10307 - The manufacturer shall make the Secure Component technical documentation accessi... implements: SPPRAMSS-5336 - Annex I-2 Vulnerability Handling Requirements implements: SPPRAMSS-5318 - Article 31- Technical documentation implements: SPPRAMSS-5460 - Article 32- Conformity assessment procedures
EU-CRA 13-13	Manufacturers shall keep the technical documentation and the EU declaration of c...	implements: SPPRAMSS-10307 - The manufacturer shall make the Secure Component technical documentation accessi...

EU CRA	Requirment	Linked Work Items
EU-CRA 13-14	Manufacturers shall ensure that procedures are in place for products with digita...	implements: SPPRAMSS-6809 - SM-12: Process verification implements: SPPRAMSS-6804 - SM-13: Continuous improvement implements: SPPRAMSS-6818 - SM-1: Development process implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-15	Manufacturers shall ensure that their products with digital elements bear a type...	implements: SPPRAMSS-10250 - How to identify the product implements: SPPRAMSS-10259 - Product Type implements: SPPRAMSS-10258 - Product Identification implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-16	Manufacturers shall indicate the name, registered trade name or registered trade...	implements: SPPRAMSS-10251 - Electronic contact address implements: SPPRAMSS-10255 - Postal address implements: SPPRAMSS-10254 - Registered trade name or trade mark implements: SPPRAMSS-10252 - Website implements: SPPRAMSS-10256 - Manufacturer name implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-17	For the purposes of this Regulation, manufacturers shall designate a single poin...	implements: SPPRAMSS-10253 - Vulnerability reporting implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA 13-18	Manufacturers shall ensure that products with digital elements are accompanied b...	implements: SPPRAMSS-6850 - SG-5: Secure operation guidelines implements: SPPRAMSS-6852 - SG-1: Product defense in depth implements: SPPRAMSS-6885 - The Secure Component documentation shall be written in an official language of t... implements: SPPRAMSS-5349 - Annex II - Information and Instructions to the User implements: SPPRAMSS-10291 - Security configuration options implements: SPPRAMSS-10272 - Initial commissioning steps implements: SPPRAMSS-10293 - Operational security tasks implements: SPPRAMSS-10281 - Decommissioning steps implements: SPPRAMSS-10277 - Maintenance activities implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-19	Manufacturers shall ensure that the end date of the support period referred to i...	implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date
EU-CRA 13-20	Manufacturers shall either provide a copy of the EU declaration of conformity or...	implements: SPPRAMSS-10270 - EU declaration of conformity implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...

EU CRA	Requirment	Linked Work Items
EU-CRA 13-21	From the placing on the market and for the support period, manufacturers who kno...	implements: SPPRAMSS-6854 - SUM-4: Security update delivery implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 13-22	Manufacturers shall, upon a reasoned request from a market surveillance authorit...	
EU-CRA 13-23	A manufacturer that ceases its operations and, as a result, is not able to compl...	implements: SPPRAMSS-6879 - If a manufacturer ceases operation, the manufacturer shall inform the relevant m...
EU-CRA 14-01	A manufacturer shall notify any actively exploited vulnerability contained in th...	implements: SPPRAMSS-6857 - DM-5: Disclosing security-related issues implements: SPPRAMSS-6859 - DM-4: Addressing security-related issues implements: SPPRAMSS-6844 - DM-3: Assessing security-related issues implements: SPPRAMSS-6840 - DM-1: Receiving notifications of security-related issues implements: SPPRAMSS-6841 - DM-2: Reviewing security-related issues implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 14-02	For the purposes of the notification referred to in paragraph 1, the manufacture...	implements: SPPRAMSS-10453 - The manufacturer shall submit a final report to the the designated CSIRT and to... implements: SPPRAMSS-10452 - The manufacturer shall submit a vulnerability information to the the designated... implements: SPPRAMSS-6881 - The manufacturer shall submit an early warning notification to the designated CS... implements: SPPRAMSS-10454 - The manufacturer shall submit an incident notification within 72h to the designa...
EU-CRA 14-03	A manufacturer shall notify any severe incident having an impact on the security...	implements: SPPRAMSS-6881 - The manufacturer shall submit an early warning notification to the designated CS...
EU-CRA 14-04	For the purposes of the notification referred to in paragraph 3, the manufacture...	implements: SPPRAMSS-10455 - The manufacturer shall submit an final within 1 month to the designated CSIRT an...
EU-CRA 14-08	After becoming aware of an actively exploited vulnerability or a severe incident...	implements: SPPRAMSS-6883 - The manufacturer shall notify without undue delay and after becoming aware, the...
EU-CRA 31-01	The technical documentation shall contain all relevant data or details of the me...	implements: SPPRAMSS-6840 - DM-1: Receiving notifications of security-related issues implements: SPPRAMSS-5468 - Annex VI - Simplified EU Declaration of Conformity

EU CRA	Requirment	Linked Work Items
EU-CRA 31-02	The technical documentation shall be drawn up before the product with digital el...	implements: SPPRAMSS-6804 - SM-13: Continuous improvement implements: SPPRAMSS-6847 - SG-7: Documentation review implements: SPPRAMSS-6884 - The manufacturer shall update the Secure Component technical documentation where... implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA 31-04	The technical documentation and correspondence relating to any conformity assess...	implements: SPPRAMSS-6885 - The Secure Component documentation shall be written in an official language of t...
EU-CRA 32-01	The manufacturer shall perform a conformity assessment of the product with digit...	
EU-CRA 32-02	Where, in assessing the compliance of an important product with digital elements...	implements: SPPRAMSS-5404 - By 12 months from the date of entry into force of this Regulation, the Commissio...
EU-CRA 32-02a	the EU-type examination procedure (based on module B) set out in Annex VIII foll...	
EU-CRA 32-02b	a conformity assessment based on full quality assurance (based on module H) set...	
EU-CRA 32-03a	EU-type examination procedure (based on module B) set out in Annex VIII followed...	
EU-CRA 32-03b	a conformity assessment based on full quality assurance (based on module H) set...	
EU-CRA 32-03c	where available and applicable, a European cybersecurity certification scheme pu...	
EU-CRA 32-3	Where the product is an important product with digital elements that falls under...	implements: SPPRAMSS-5404 - By 12 months from the date of entry into force of this Regulation, the Commissio...
EU-CRA Annex I-1.1	(1) Products with digital elements shall be designed, developed and produced in...	implements: SPPRAMSS-6826 - SR-4 Product security requirements content implements: SPPRAMSS-6828 - SR-2 Threat model implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-1.2a	Products with digital elements shall shall be made available on the market witho...	implements: SPPRAMSS-6836 - SVV-3: Vulnerability testing implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-1.2b	Products with digital elements shall be made available on the market with a secu...	implements: SPPRAMSS-6748 - The Secure Component shall provide the maintenance method Security:FactoryReset(... implements: SPPRAMSS-6886 - The Secure Component shall have a factory configuration that is secure by defaul...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex I-1.2c	Products with digital elements shall ensure that vulnerabilities can be addresse...	implements: SPPRAMSS-2497 - The Secure Component shall support the update of software and configuration via...
EU-CRA Annex I-1.2d	Products with digital elements shall ensure protection from unauthorised access...	implements: SPPRAMSS-3999 - The Secure Component shall authenticate each communication partner by validating...
EU-CRA Annex I-1.2f	Products with digital elements shall protect the integrity of stored, transmitte...	implements: ~~SPPRAMSS-2479~~ - The Secure Component shall protect the integrity of data in transit.
EU-CRA Annex I-1.2g	Products with digital elements shall process only data, personal or other, that...	implements: SPPRAMSS-6676 - If the Secure Component uses the standard communication protocols defined in , t...
EU-CRA Annex I-1.2h	Products with digital elements shall protect the availability of essential and b...	implements: SPPRAMSS-6612 - Refine requirement of not adversely affect essential functions
EU-CRA Annex I-1.2i	Products with digital elements shall minimise the negative impact by the product...	implements: SPPRAMSS-2555 - The Secure Component's host-based firewall filter shall be capable of filtering... implements: SPPRAMSS-3822 - The Secure Component shall provide the capability of a host-based firewall (e.g.... implements: SPPRAMSS-3821 - The host-based firewall shall deny by default all inbound and outbound connectio... implements: SPPRAMSS-3779 - The Secure Component shall implement the hardening measures according to the rel...
EU-CRA Annex I-1.2j	Products with digital elements shall be designed, developed and produced to limi...	implements: SPPRAMSS-2621 - The supplier shall deactivate unused interfaces. implements: SPPRAMSS-3779 - The Secure Component shall implement the hardening measures according to the rel...
EU-CRA Annex I-1.2j	Products with digital elements shall provide security related information by rec...	implements: SPPRAMSS-2581 - The Secure Component shall log at least the following events:
EU-CRA Annex I-1.2k	Products with digital elements shall be designed, developed and produced to redu...	implements: SPPRAMSS-6832 - SD-2: Defense in depth design implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-1.2m	Products with digital elements shall provide the possibility for users to secure...	implements: SPPRAMSS-10281 - Decommissioning steps
EU-CRA Annex I-1.3e	Products with digital elements shall protect the confidentiality of stored, tran...	implements: SPPRAMSS-3013 - If read access authorisation to persistent data is required, the Secure Componen... implements: SPPRAMSS-6676 - If the Secure Component uses the standard communication protocols defined in , t... implements: SPPRAMSS-6887 - The Secure Component shall provide the capability to use encryption ciphers for...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex I-2.1	Manufacturers of the products with digital elements shall identify and document...	implements: SPPRAMSS-5399 - The Commission may, by means of implementing acts taking into account European o... implements: SPPRAMSS-6840 - DM-1: Receiving notifications of security-related issues implements: SPPRAMSS-6888 - The manufacturer shall create a software bill of materials using the CycloneDX S... implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-2.2	Manufacturers of the products with digital elements shall in relation to the ris...	implements: SPPRAMSS-6854 - SUM-4: Security update delivery implements: SPPRAMSS-6859 - DM-4: Addressing security-related issues implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-2.3	Manufacturers of the products with digital elements shall apply effective and re...	implements: SPPRAMSS-6838 - SVV-1: Security requirements testing implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-2.4	Manufacturers of the products with digital elements shall once a security update...	implements: SPPRAMSS-6854 - SUM-4: Security update delivery implements: SPPRAMSS-6857 - DM-5: Disclosing security-related issues implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex I-2.5	Manufacturers of the products with digital elements shall put in place and enfor...	implements: SPPRAMSS-5411 - Manufacturers shall ensure, when placing a product with digital elements on the... implements: SPPRAMSS-10249 - Vulnerability reporting policy
EU-CRA Annex I-2.6	Manufacturers of the products with digital elements shall take measures to facil...	implements: SPPRAMSS-10247 - Vulnerability information
EU-CRA Annex I-2.7	Manufacturers of the products with digital elements shall provide for mechanisms...	implements: SPPRAMSS-6851 - SUM-5: Timely delivery of security patches implements: SPPRAMSS-2982 - The Secure Component shall verify the signature of the update packages using the... implements: SPPRAMSS-4028 - The update package shall be signed using the corresponding update signing key (c... implements: SPPRAMSS-6892 - The manufacturer shall provide for mechanisms to securely distribute updates for... implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex I-2.8	Manufacturers of the products with digital elements shall ensure that, where sec...	implements: SPPRAMSS-6851 - SUM-5: Timely delivery of security patches implements: SPPRAMSS-6893 - The manufacturer shall provide the security patches or updates without undue del... implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex II-1	1. the name, registered trade name or registered trademark of the manufacturer,...	implements: SPPRAMSS-10251 - Electronic contact address implements: SPPRAMSS-10250 - How to identify the product implements: SPPRAMSS-10255 - Postal address implements: SPPRAMSS-10254 - Registered trade name or trade mark implements: SPPRAMSS-10252 - Website implements: SPPRAMSS-10258 - Product Identification implements: SPPRAMSS-10256 - Manufacturer name implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-2	2. the single point of contact where information about vulnerabilities of the pr...	implements: SPPRAMSS-10247 - Vulnerability information implements: SPPRAMSS-10249 - Vulnerability reporting policy implements: SPPRAMSS-10253 - Vulnerability reporting implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-3	3. name and type and any additional information enabling the unique identificati...	implements: SPPRAMSS-2998 - The security seal shall contain a number unique to the supplier. implements: SPPRAMSS-6895 - The Secure Component encasing shall include the type, batch, version or serial n... implements: SPPRAMSS-10261 - Product Version implements: SPPRAMSS-10260 - Product Name implements: SPPRAMSS-10259 - Product Type implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-4	4. the intended purpose of the product with digital elements, including the secu...	implements: SPPRAMSS-6848 - SG-2: Defense in depth measures expected in the environment implements: SPPRAMSS-6852 - SG-1: Product defense in depth implements: SPPRAMSS-10267 - Provided security environment implements: SPPRAMSS-10266 - Indented purpose of the product implements: SPPRAMSS-10264 - Essential functions of the product implements: SPPRAMSS-10265 - Security standards compliance implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex II-5	5. any known or foreseeable circumstance, related to the use of the product with...	implements: SPPRAMSS-6850 - SG-5: Secure operation guidelines implements: SPPRAMSS-10269 - Security risks implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-6	6. where applicable, the internet address at which the EU declaration of conform...	implements: SPPRAMSS-10270 - EU declaration of conformity implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-7	7. the type of technical security support offered by the manufacturer and the en...	implements: SPPRAMSS-10274 - Technical Security support implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8	9. detailed instructions or an internet address referring to such detailed instr...	implements: SPPRAMSS-10272 - Initial commissioning steps implements: SPPRAMSS-10277 - Maintenance activities implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8a	(a) the necessary measures during initial commissioning and throughout the lifet...	implements: SPPRAMSS-6852 - SG-1: Product defense in depth implements: SPPRAMSS-10272 - Initial commissioning steps implements: SPPRAMSS-10277 - Maintenance activities implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8b	(b) how changes to the product with digital elements can affect the security of...	implements: SPPRAMSS-6852 - SG-1: Product defense in depth implements: SPPRAMSS-10278 - Changes affecting security implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8c	(c) how security-relevant updates can be installed;	implements: SPPRAMSS-6856 - SUM-2: Security update documentation implements: SPPRAMSS-10279 - Installing security updates implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex II-8d	(d) the secure decommissioning of the product with digital elements, including i...	implements: SPPRAMSS-6845 - SG-4: Secure disposal guidelines implements: SPPRAMSS-10281 - Decommissioning steps implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8e	how the default setting enabling the automatic installation of security updates,...	implements: SPPRAMSS-10282 - Disable automatic security update implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-8f	where the product with digital elements is intended for integration into other p...	implements: SPPRAMSS-10283 - Expected security environment / Security related application conditions implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex II-9	If the manufacturer decides to make available the software bill of materials to...	implements: SPPRAMSS-10284 - Software Bill of Material: implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex VI-2.3	Design, development, production and vulnerability handling of products with digi...	
EU-CRA Annex VI-2.3.2	3.2. The quality system shall ensure compliance of the products with the essenti...	
EU-CRA Annex VI-2.3.6	3.6 or whether a reassessment is necessary.	
EU-CRA Annex VI-2.4	4. Surveillance under the responsibility of the notified body	
EU-CRA Annex VI-2.4.1	4.1. The purpose of surveillance is to make sure that the manufacturer duly fulf...	
EU-CRA Annex VI-2.5	5. Conformity marking and declaration of conformity	
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	Requirment	Linked Work Items
EU-CRA Annex VII-1b	(b) versions of software affecting compliance with essential cybersecurity requi...	
EU-CRA Annex VII-1c	(c) where the product with digital elements is a hardware product, photographs o...	
EU-CRA Annex VII-1d	(d) user information and instructions as set out in Annex II;	implements: SPPRAMSS-5372 - (c) necessary information and specifications of the production and monitoring pr...
EU-CRA Annex VII-2	2. a description of the design, development and production of the product with d...	implements: SPPRAMSS-6808 - SM-11: Assessing and addressing security-related issues implements: SPPRAMSS-6844 - DM-3: Assessing security-related issues implements: SPPRAMSS-6840 - DM-1: Receiving notifications of security-related issues implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex VII-2a	(a) necessary information on the design and development of the product with digi...	implements: SPPRAMSS-6886 - The Secure Component shall have a factory configuration that is secure by defaul... implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex VII-2b	(b) necessary information and specifications of the vulnerability handling proce...	implements: SPPRAMSS-6841 - DM-2: Reviewing security-related issues implements: SPPRAMSS-6844 - DM-3: Assessing security-related issues implements: SPPRAMSS-6859 - DM-4: Addressing security-related issues implements: SPPRAMSS-6857 - DM-5: Disclosing security-related issues implements: SPPRAMSS-6858 - DM-6: Periodic review of security defect management practice implements: SPPRAMSS-6809 - SM-12: Process verification
EU-CRA Annex VII-2c	(c) necessary information and specifications of the production and monitoring pr...	implements: SPPRAMSS-5376 - (d) user information and instructions as set out in Annex II;
EU-CRA Annex VII-3	3. an assessment of the cybersecurity risks against which the product with digit...	implements: SPPRAMSS-6828 - SR-2 Threat model implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex VII-4	4. relevant information that was taken into account to determine the support per...	implements: SPPRAMSS-10273 - Vulnerability handling and security update end-date
EU-CRA Annex VII-5	5. a list of the harmonised standards applied in full or in part the references...	implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...

EU CRA	Requirment	Linked Work Items
EU-CRA Annex VII-6	6.reports of the tests carried out to verify the conformity of the product with...	implements: SPPRAMSS-6838 - SVV-1: Security requirements testing implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex VII-7	7. a copy of the EU declaration of conformity;	implements: SPPRAMSS-10270 - EU declaration of conformity implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex VII-8	8. where applicable, the software bill of materials, further to a reasoned reque...	implements: SPPRAMSS-10284 - Software Bill of Material: implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex VIII-P1-2	The manufacturer shall draw up the technical documentation described in Annex VI...	implements: SPPRAMSS-6894 - The Secure Component shall include the information set out in the in a document...
EU-CRA Annex VIII-P1-3	Design, development, production and vulnerability handling of products with digi...	implements: SPPRAMSS-2495 - The Secure Component shall be developed according to IEC 62443-4-1 (maturity lev...
EU-CRA Annex VIII-P1-4.1	The manufacturer shall affix the CE marking to each individual product with digi...	
EU-CRA Annex VIII-P1-4.2	The manufacturer shall draw up a written EU declaration of conformity for each p...	implements: SPPRAMSS-10270 - EU declaration of conformity
EU-CRA Annex VIII-P1-5	The manufacturer’s obligations set out in point 4 may be fulfilled by its author...	
EU-CRA Annex VIII-P2-01	1. EU-type examination is the part of a conformity assessment procedure in which...	
EU-CRA Annex VIII-P2-02	2. EU-type examination shall be carried out by assessment of the adequacy of the...	
EU-CRA Annex VIII-P2-03	3. The manufacturer shall lodge an application for EU-type examination with a si...	
EU-CRA Annex VIII-P2-03.1	The application shall include the name and address of the manufacturer and, if t...	

EU CRA	Requirment	Linked Work Items
EU-CRA Annex VIII-P2-03.2	The application shall include a written declaration that the same application ha...	
EU-CRA Annex VIII-P2-03.3	The application shall include the technical documentation, which shall make it p...	
EU-CRA Annex VIII-P2-03.4	The application shall include the supporting evidence for the adequacy of the te...	
EU-CRA Annex VIII-P2-04.1	The notified body shall examine the technical documentation and supporting evide...	
EU-CRA Annex VIII-P2-04.2	The notified body shall verify that specimens have been developed or manufacture...	
EU-CRA Annex VIII-P2-04.3	The notified body shall carry out appropriate examinations and tests, or have th...	
EU-CRA Annex VIII-P2-04.4	The notified body shall carry out appropriate examinations and tests, or have th...	
EU-CRA Annex VIII-P2-04.5	The notified body shall agree with the manufacturer on a location where the exam...	
EU-CRA Annex VIII-P2-05	The notified body shall draw up an evaluation report that records the activities...	
EU-CRA Annex VIII-P2-06	Where the type and the vulnerability handling processes meet the essential cyber...	
EU-CRA Annex VIII-P2-07	The notified body shall keep itself apprised of any changes in the generally ack...	
EU-CRA Annex VIII-P2-08	The notified body shall carry out periodic audits to ensure that the vulnerabili...	

EU CRA	Requirment	Linked Work Items
EU-CRA Annex VIII-P2-09	Each notified body shall inform its notifying authorities concerning the EU-type...	
EU-CRA Annex VIII-P2-10	9. The manufacturer shall keep a copy of the EU-type examination certificate, it...	
EU-CRA Annex VIII-P2-11	10. The manufacturer's authorised representative may lodge the application refer...	
EU-CRA Annex VIII-P3-3.1	The manufacturer shall affix the CE marking to each individual product with digi...	
EU-CRA Annex VIII-P3-3.2	The manufacturer shall draw up a written declaration of conformity for a product...	
EU-CRA Annex VIII-P3-4	The manufacturer's obligations set out in point 3 may be fulfilled by its author...	
EU-CRA Annex VIII-P4-1	Conformity based on full quality assurance is the conformity assessment procedur...	
EU-CRA Annex VIII-P4-2	The manufacturer shall operate an approved quality system as specified in point...	
EU-CRA Annex VIII-P4-2	2. Design, development, production and vulnerability handling of products with d...	
EU-CRA Annex VIII-P4-3.1	The manufacturer shall lodge an application for assessment of its quality system...	
EU-CRA Annex VIII-P4-3.1a	The application shall include the name and address of the manufacturer and, if t...	
EU-CRA Annex VIII-P4-3.1b	The application shall includethe technical documentation for one model of each c...	

EU CRA	Requirment	Linked Work Items
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 ha...	
EU-CRA Annex VIII-P4-3.2	The quality system shall ensure compliance of the products with digital elements...	
EU-CRA Annex VIII-P4-3.2a	– the quality objectives and the organisational structure, responsibilities and...	
EU-CRA Annex VIII-P4-3.2b	– the technical design and development specifications, including standards, that...	
EU-CRA Annex VIII-P4-3.2c	– the procedural specifications, including standards, that will be applied and,...	
EU-CRA Annex VIII-P4-3.2d	– the design and development control, as well as design and development verifica...	
EU-CRA Annex VIII-P4-3.2e	–the design and development control, as well as design and development verificat...	
EU-CRA Annex VIII-P4-3.2f	– the examinations and tests that will be carried out before, during and after p...	
EU-CRA Annex VIII-P4-3.2g	– the quality records, such as inspection reports and test data, calibration dat...	
EU-CRA Annex VIII-P4-3.2h	– the means of monitoring the achievement of the required design and product qua...	
EU-CRA Annex VIII-P4-3.3	3.3. The notified body shall assess the quality system to determine whether it s...	

EU CRA	Requirment	Linked Work Items
EU-CRA Annex VIII-P4-3.4	The manufacturer shall undertake to fulfil the obligations arising out of the qu...	
EU-CRA Annex VIII-P4-3.5	The manufacturer shall keep the notified body that has approved the quality syst...	
EU-CRA Annex VIII-P4-3.5	The purpose of surveillance is to make sure that the manufacturer duly fulfils	
EU-CRA Annex VIII-P4-4.1	The purpose of surveillance is to make sure that the manufacturer duly fulfils t...	
EU-CRA Annex VIII-P4-4.2	The manufacturer shall, for assessment purposes, allow the notified body access...	
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,...	
EU-CRA Annex VIII-P4-4.2c	– the quality records as provided for by the manufacturing part of the quality s...	
EU-CRA Annex VIII-P4-4.3	The notified body shall carry out periodic audits to make sure that the manufact...	
EU-CRA Annex VIII-P4-5.1	The manufacturer shall affix the CE marking, and, under the responsibility of th...	
EU-CRA Annex VIII-P4-5.2	The manufacturer shall draw up a written declaration of conformity for each prod...	
EU-CRA Annex VIII-P4-6	The manufacturer shall, for a period ending at least 10 years after the product...	

EU CRA	Requirment	Linked Work Items
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...	
EU-CRA Annex VIII-P4-8	The manufacturer's obligations set out in points 3.1, 3.5, 5 and 6 may be fulfil...	

163 items found

(type:srq AND (oldID:EU\-CRA AND NOT status:deleted)) AND project.id:SPPRAMS

[Open, SPPRAMSS-7309]

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

This section will be filled in the next version of this document.

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

Norm ID	Requirement	Linked Work Items
TS 50701 - 7.2.10b	List of detailed security requirements, including SL-T, assumptions and security...	implements: SPPRAMSS-1460 - List of detailed security requirements
TS 50701 - 7.2.10c	SuC description (see 6.2)	implements: SPPRAMSS-2286 - The generic security architecture is defined in .
TS 50701 - 7.2.10d	Zone or conduit drawings (see 6.4)	implements: SPPRAMSS-2289 - The zone and conduits are defined in
TS 50701 - 7.2.10e	Zone or conduit characteristics (see 6.4)	implements: SPPRAMSS-2288 - The zone and conduits characteristics are defined in

Norm ID	Requirement	Linked Work Items
TS 50701 - 7.2.10f	Operating environment assumptions (see 6.2 and 7.2.4.4.3)	implements: SPPRAMSS-4889 - It is assumed that the Secure Component is operated and maintained by an organiz... implements: SPPRAMSS-4900 - It is assumed that a Secure Component is installed in an housing with physical a... implements: SPPRAMSS-4890 - It is assumed that a Secure Component has access to the shared security services...
TS 50701 - 7.2.10g	Threat environment (see 6.2 and 7.2.1)	implements: SPPRAMSS-6611 - add reference to risk analyses
TS 50701 - 7.2.10h	Risk Acceptance (see 6.5.3)	implements: SPPRAMSS-7014 - Regulatory requirements
TS 50701 - 7.2.10i	Regulatory requirements	implements: SPPRAMSS-7018 - Risk Acceptance (see 6.5.3)
TS 50701 - 7.2.10k	Cybersecurity requirements and security-related application conditions shall be...	
TS 50701 - 7.2.10l	For requirement tracing, cybersecurity requirements that are necessary to protec...	implements: SPPRAMSS-7027 - Identifying security requirements protecting essential functions
10 items found		

to be done when updated version is available (eg. Q4 2025)
Table containing IEC 63452 req no, title and corresponding req or chapter in this doc