EU-RAIL SYSTEM PILLAR

Secure Component Specification

Secure Component Specification

Author(s)	Wischy, Markus Alexander (SMO RI R&D F IL) , SISIARIDIS Dimitrios , Max Schubert , POYET Nicolas , Richard Poschinger , David Goltzsche , WELLER Martin
Abstract	Component-specific Security Requirements
Config Item	System Requirements Specification
Document ID	Main Documents/SP-SEC-CompSpec#828042 Secure Component Specification
Classification	Public
Status	In Decision by Steering Group
Version	1.1
Revision	828042
Last Change Date	17.02.2026
Copyright	Brussels: Europe’s Rail Joint Undertaking, 2026

Document History

Draft for Innovation Pillar and sync with other domains 28.06.2023	Wischy, Markus Alexander (SMO RI R&D SYS SEC)	Approved version based on Review X.X
V1.0 (release canditate) 21.01.2025	Wischy, Markus Alexander (SMO RI R&D F IL)	Reviewed version including Change Request
V1.0 05.02.2025	Goltzsche, David (SMO RI R&D F SEC)	Approved version based on Review V1.0 (release canditate)
1.0 25.09.2025	Jorge Block	Approved version based on Review V1.0
1.1 16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9

1.0.9	23.01.2026	Goltzsche, David (SMO RI R&D F SEC)	Reviewed version including Findings from Review 1.1
1.1	16.02.2026	David Goltzsche	Reviewed version including Findings from Review 1.0.9

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

Approval by reviewers

Type of Approval	🔍 Document Review

Approval by approvers

Type of Approval	✓ Document Approval

1 Table of Contents

2 Preamble

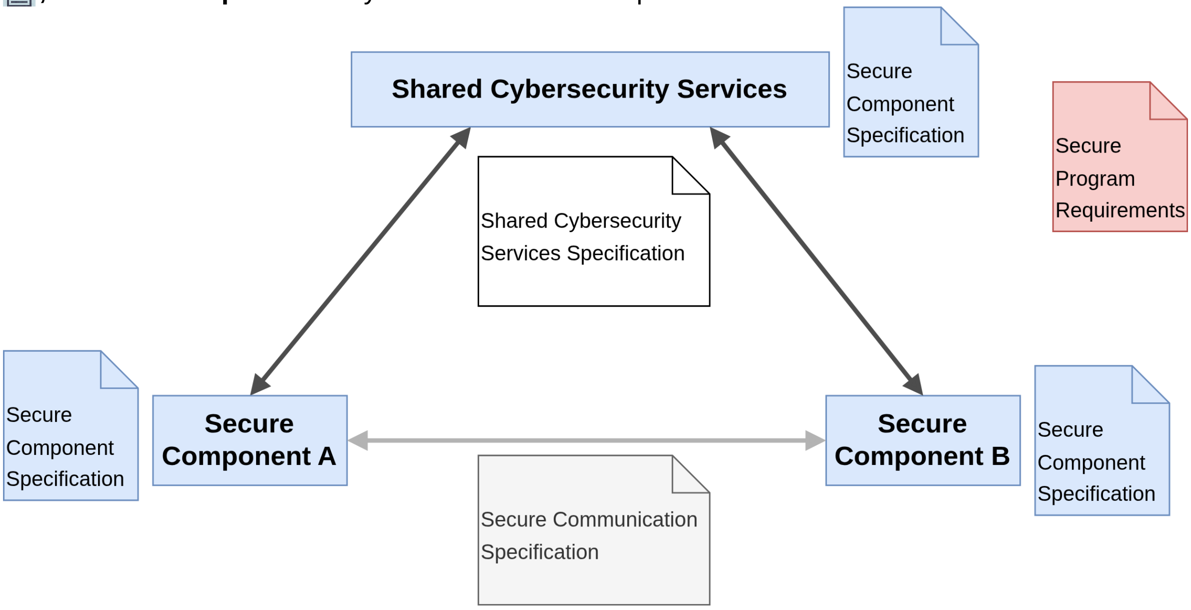
2.1 Scope, Purpose and Intended Audience

🗎, **SP-SEC-Comp-2.1-1 -** This specification is a Cybersecurity Requirements Specification (CRS) according with [IEC 62443-3-2:2020], [CEN-CENELEC TS 50701:2023] and [IEC PT 63452] **[**SPPRAMSS-9659 **]**

🗎, **SP-SEC-Comp-2.1-2 -** This CRS is intended to be 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). **[**SPPRAMSS-9646 **]**

🗎, **SP-SEC-Comp-2.1-3 -** The following figure shows the relationship of this specification to the key terms and other referenced specifications. **[**SPPRAMSS-9647 **]**

🗎, **SP-SEC-Comp-2.1-4 -** Key terms and technical specs used in 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

[SPPRAMSS-7034 **]**

🗎, **SP-SEC-Comp-2.1-5 -** In particular this CRS does not define:
· Detailed requirements for Secure Communication. These requirements can be found in the Secure Communication Specification [SP-SEC-CommSpec] .
· Requirements for the interfaces to the shared cybersecurity services. These requirements can be found in the Shared Cybersecurity Services Specification [SP-SEC-ServSpec]
· Security life-cycle requirements, including operational requirements. These requirements can be found in the Security Program Requirements [SP-SEC-PrgmReq].
[SPPRAMSS-9626 **]**

🗎, **SP-SEC-Comp-2.1-6 -** The Secure Component specification has been specified to be used together with the Shared Cybersecurity Services Specification and the Secure Communication Specification. **[**SPPRAMSS-9628 **]**

🗎, **SP-SEC-Comp-2.1-7 -** 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 specification with the component type "Network Component" (see definiton Network Component). **[**SPPRAMSS-9630 **]**

, **SP-SEC-Comp-2.1-8 -** 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 Machine Interface (e.g. a component with a screen and interaction capabilities as keyboard, mouse, touch,...). See definition HMI Component.
- Requirements with component type "Wireless" is only applicable for components with a wireless communication interfaces (e.g. IEEE 802.11, GSM, 5G, FRMCS,...). See definition Wireless Component.
- Requirements with component type "Network" are applicable only for network components (see definition Network Component.

[SPPRAMSS-9621 **]**

2.2 Document usage

, **SP-SEC-Comp-2.2-1 -** This specification includes all requirements required for protection against threats defined in the generic risk assessment performed on the generic security architecture (see SP-SEC-CompSpec Ch 4.2.7 - Threat and risk analysis result) and to achieve compliance to various standards (see [Document base]). **[**SPPRAMSS-9636 **]**

, **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. **[**SPPRAMSS-10321 **]**

, **SP-SEC-Comp-2.2-3 -** If a requirement of this specification cannot be implemented (yet), the component documentation shall provide a justification for each non-implemented requirement, with respect to organisational needs, operational constraints and regulatory requirements (e.g. interface is not needed for operation, alternative mitigation, justified by an impact / risk analysis). **[**Generic , SPPRAMSS-9637 **]**

, **SP-SEC-Comp-2.2-4 -** If a requirement of this specification cannot be implemented (yet), the component documentation shall include a description how to handle this case which has to be agreed with the asset owner (e.g. definition of a security related application condition). **[**Generic , SPPRAMSS-9638 **]**

, **SP-SEC-Comp-2.2-5 -** This specification uses identifiers starting with "SP-SEC-Comp". **[**SPPRAMSS-13356 **]**

, **SP-SEC-Comp-2.2-6 -** References, taxonomy, key terms, and icon types used in this document are defined in [SP-SEC-Tax]. **[**SPPRAMSS-13857 **]**

2.3 References

, **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. **[**SPPRAMSS-14017 **]**

- [SP-SEC-Tax]
Europe's Rail System Pillar Cybersecurity Domain - Taxonomy and References, v1.1

- [Document base]
This CRS was developed based on:

- [IEC 62443-4-2:2019]
- [EULYNX/EU-Rail BL4 R3]
- ESCG Requirements
- [UNISIG SUBSET-146 v4.00]
- [UNISIG SUBSET-147 v4.00]
- [CEN-CENELEC TS 50701:2023] and
- [IEC PT 63452] (draft version Jan 2025)

- [SP-SEC-InitRiskAna]
Europe's Rail System Pillar Cybersecurity Domain - Intial Risk Analysis, v1.1

- [SP-SEC-ThreatCat]
Europe's Rail System Pillar Cybersecurity Domain - Threat Catalog, v1.1

- [SP-SEC-DocTempl]
Europe's Rail System Pillar Cybersecurity Domain - Product Documentation Template, v1.1

- [SP-SEC-CompSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.1

- [SP-SEC-CommSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.1

- [SP-SEC-ServSpec]
Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.1

- [SP-SEC-PrgmReq]
Europe's Rail System Pillar Cybersecurity Domain - Secure Program Requirements, v1.1

- [RFC 4086]
Randomness Requirements for Security

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

- [MinElements_SBOM]
The Minimum Elements for an SBOM

- [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

2.4 Acronyms and Abbreviations

Acronym (abbreviation)	Full text (title)
ATO	Automatic Train Operation
DNS	Domain Name System
HMI	Human Machine Interface
PKI	Public Key Infrastructure
VLAN	Virtual Local Area Network
CCS	Control Command and Signaling
CPU	Central Processing Unit
EU	European Union
ETCS	European Train Control System
RBC	Radio Block Centre
SSI	Standard Security Interface
PKCS #10	Certification Request Standard
CMP	Certificate Management Protocol
COTS	Commercial-off-the-shelf
CRA	Cyber Resilience Act
CRL	Certificate Revocation List
CRS	Cybersecurity Requirement Specification
DMZ	Demilitarized Zone
DoS	Denial of Service
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation
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
SBOM	Software Bill of Material
SC	Secure Component
SCS	Shared Cybersecurity Services
SNMP	Simple Network Management Protocol
SUC	System Under Consideration

Acronym (abbreviation)	Full text (title)
TS	Trackside
WLAN	Wireless Local Area Network

2.5 Terms and Definitions

, SP-SEC-Comp-2.5-1 - Secure Component

An implementation, as part of an automation control system, which comprises one or more host devices, embedded devices, network devices or software applications on host devices. A secure component realizes subsystem functions, implements security capabilities, consists of a physical encasing, computing capabilities and network communication, and interfaces 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, 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. [SPPRAMSS-1447]

, SP-SEC-Comp-2.5-2 - Shared Cybersecurity Services

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) implements the requirements of the Secure Component Specification as they are considered as Secure Components as well.

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

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

, SP-SEC-Comp-2.5-3 - Enterprise Cybersecurity Services

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.

Note: Enterprise Shared Services and Shared Cybersecurity Services are separated by the IT/OT border (e.g. by a DMZ). [SPPRAMSS-6720]

, SP-SEC-Comp-2.5-4 - Network Component

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

, SP-SEC-Comp-2.5-5 - 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 IEC 62443-4-2 NDR 1.6, NDR 1.6 RE1 and CR 2.2, CR 2.2 RE1) **[**SPPRAMSS-4721 **]**

, SP-SEC-Comp-2.5-6 - HMI Component

A Secure Component with a human 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-2.5-7 - Essential Function

Function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control (definition from IEC 62443-4-2)

Note: 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-13943 **]**

, SP-SEC-Comp-2.5-8 - 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-13942 **]**

3 Intentionally left blank

Intentionally left blank.

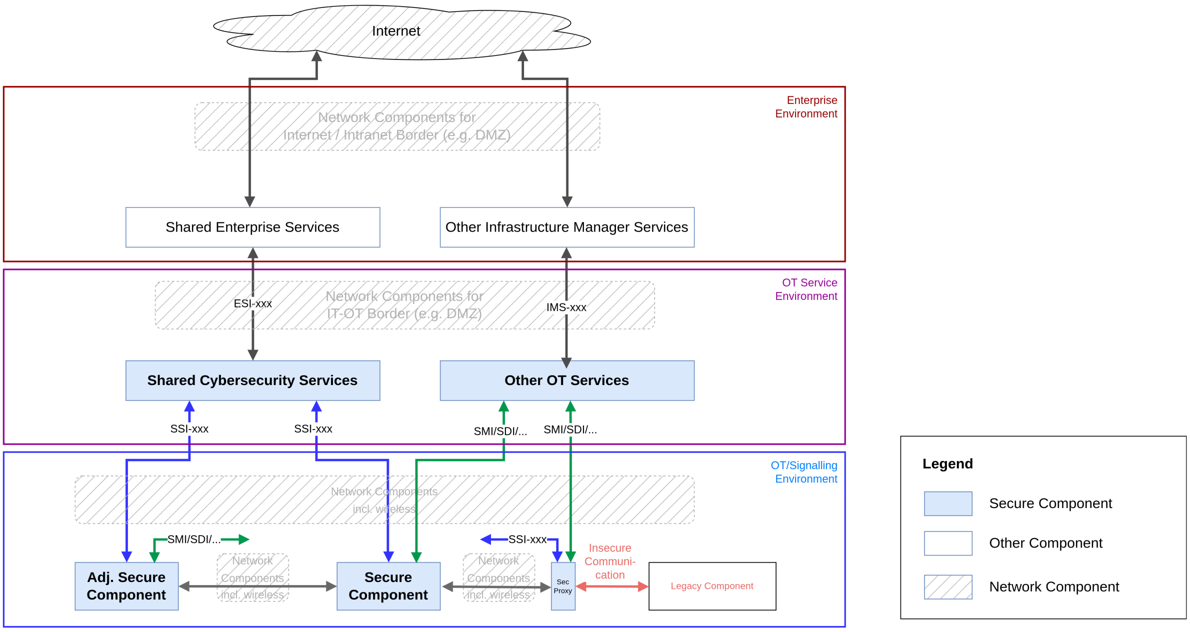
4 Component Description

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-06-01.

4.1 General SuC Description

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

, **SP-SEC-Comp-4.1-2 -** The Secure Components are shown in blue color in the figure below.


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

[SPPRAMSS-10370 **]**

4.1.1 SuC Scope and Boundary

, **SP-SEC-Comp-4.1.1-1 -** The Secure Component, as per definition SP-SEC-CompSpec Ch 3.5 - Secure Component , has a physical encasing which defines the SuC boundary, and has computing and network communication capabilities. **[**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. **[**SPPRAMSS-10379 **]**

, **SP-SEC-Comp-4.1.1-3 -** Enterprise environments, also called back-office environments, and cloud environments are outside the scope of Secure Components. These environments adhere to different security standards and specifications. However, if applications or services within the back office or cloud environment are part of the rail domain, the Shared Cybersecurity Services interfaces and parts of this specification may be applicable. **[**SPPRAMSS-10377 **]**

📄**, SP-SEC-Comp-4.1.1-4 -** Train components that do not reside in the signaling environment are outside the scope of Secure Components specification. Modern trains integrate hundreds of components from a numerous suppliers which 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. **[**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… **[**SPPRAMSS-10371 **]**

4.1.2 High-level Description

📄**, 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. **[**SPPRAMSS-10382 **]**

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

4.1.3 Interfaces of the SuC

📄**, SP-SEC-Comp-4.1.3-1 -** A Secure Component has the following interfaces:

1. Interfaces to a adjacent Secure Components via protocols defined in SecCommSpec
2. Interfaces to Shared Cybersecurity Services, specified in [SP-SEC-ServSpec] - Shared Cybersecurity Services interface specification. Usage of SSI between the SCS is not mandatory, but recommended.
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 SP-SEC-CommSpec Ch. 4 - Secure Communication for OPC UA
4. All other interfaces, for which SP-SEC-CommSpec Ch 6- Securing other communicating interfaces is applicable

[SPPRAMSS-10381 **]**

4.1.4 Support for Essential Functions

📄**, 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).

[SPPRAMSS-10384 **]**

4.2 Component Security Context

4.2.1 Generic Architecture

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

4.2.2 Mapping to Specific Architecture

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

, **SP-SEC-Comp-4.2.2-2 -** 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] .

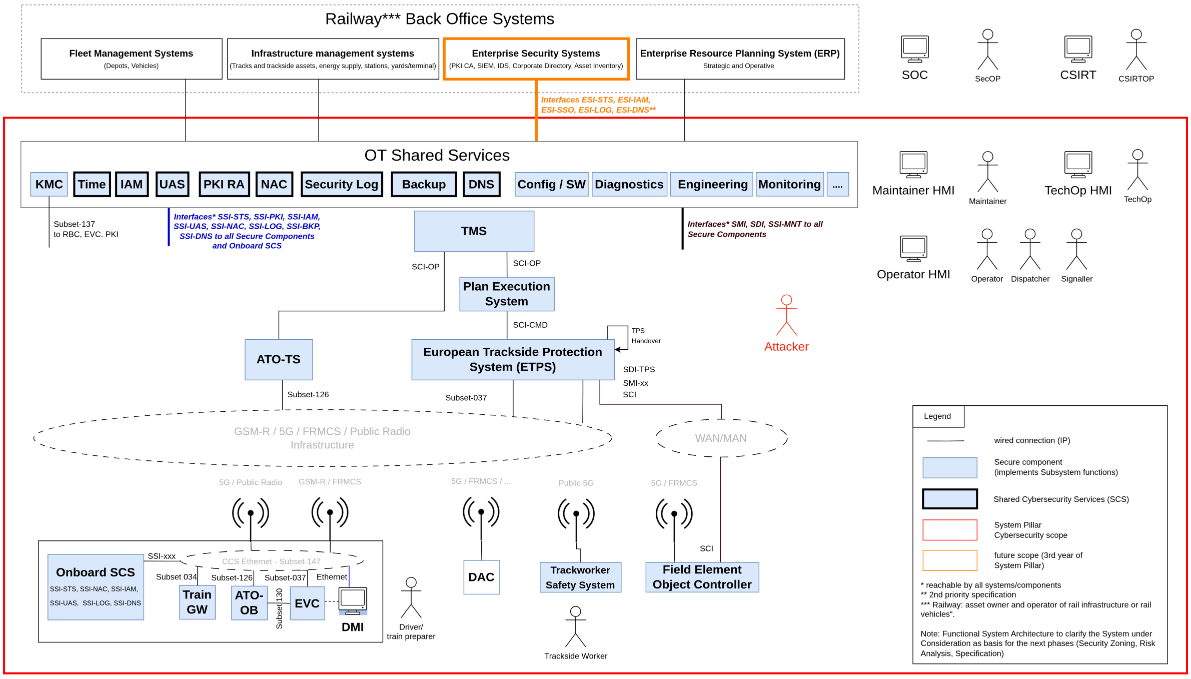

Railway*** Back Office Systems
Fleet Management Systems
(Depots, Vehicles)
Infrastructure management systems
(Tracks and trackside assets, energy supply, stations, yards/terminal)
Enterprise Security Systems
(PKI CA, SIEM, IDS, Corporate Directory, Asset Inventory)
Enterprise Resource Planning System (ERP)
Strategic and Operative
SOC
SecOP
CSIRT
CSIRTOP
Interfaces ESI-STS, ESI-IAM, ESI-SSO, ESI-LOG, ESI-DNS**
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
SCI
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/
train preparer
DAC
Trackworker Safety System
Trackside Worker
Field Element Object Controller
Legend
wired connection (IP)
Secure component
(implements Subsystem functions)
Shared Cybersecurity Services (SCS)
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)

Figure 1: Cybersecurity Architecture example based on System Pillar Traffic CS System Concept

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. **[**SPPRAMSS-13309 **]**

4.2.3 Zone and Conduits Drawing

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

, **SP-SEC-Comp-4.2.3-2 -** Generic Security Zoning

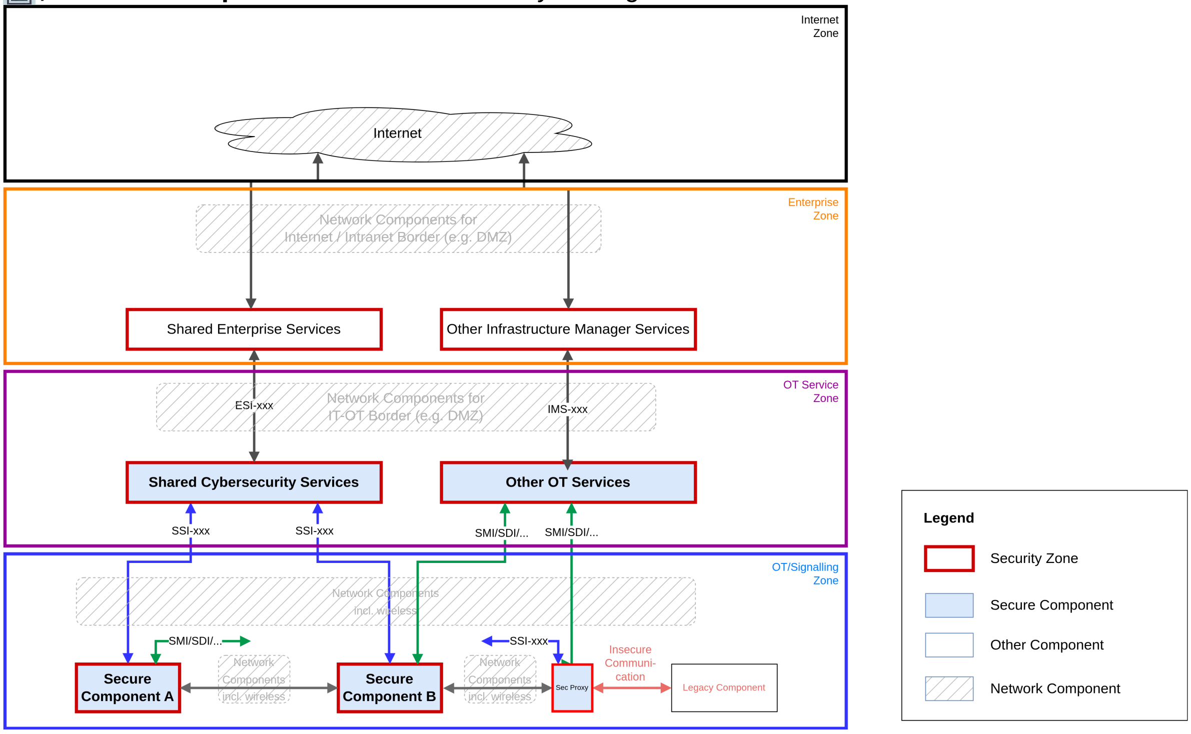


Figure 2 Generic Security Zoning

[SPPRAMSS-10392 **]**

, **SP-SEC-Comp-4.2.3-3 -** The smallest security zone can be the Secure Component itself. The Secure Component is contained in a 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 - Interfaces of the SuC . **[**SPPRAMSS-10407 **]**

, **SP-SEC-Comp-4.2.3-4 -** A special security zone is the legacy component zone. In order to interface with Secure Components, a Security Proxy implementing this specification can be used. As this zone uses insecure communication (i.e. communication without authentication or integrity protection), additional physical security measures are typically required. **[**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. **[**SPPRAMSS-11976 **]**

, **SP-SEC-Comp-4.2.3-6 -** 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. **[**SPPRAMSS-10406 **]**

, **SP-SEC-Comp-4.2.3-7 -** Example of a Security Zoning (rail automation system), where each component has its own zone. Zones could also include several components, especially when the components are co-located.

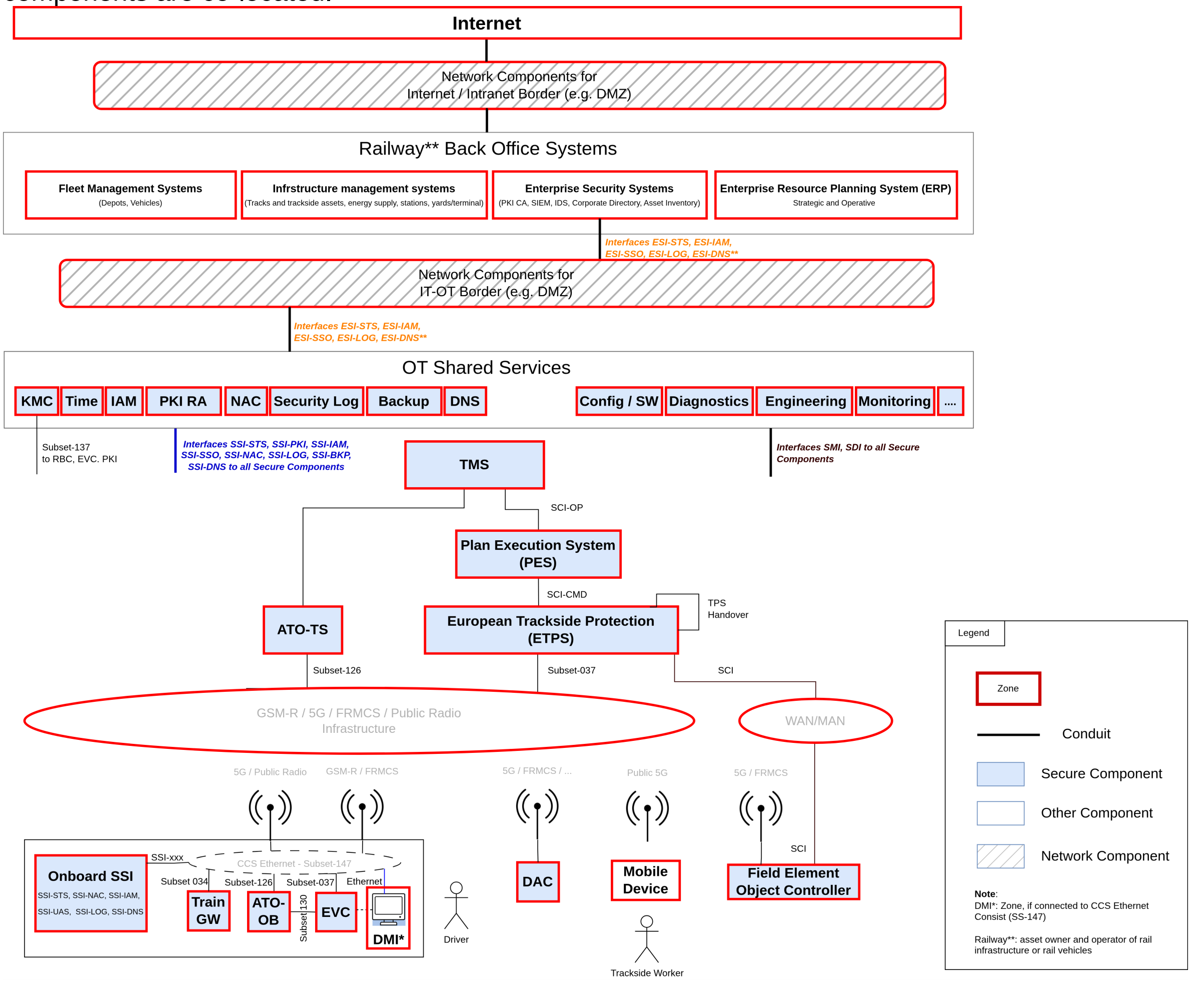

Internet
Network Components for
Internet / Intranet Border (e.g. DMZ)
Railway** Back Office Systems
Fleet Management Systems
(Depots, Vehicles)
Infrstructure management systems
(Tracks and trackside assets, energy supply, stations, yards/terminal)
Enterprise Security Systems
(PKI CA, SIEM, IDS, Corporate 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
Subset 130
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

Figure 3 Example of a Security Zoning

[SPPRAMSS-10391 **]**

4.2.4 Zone and Conduits Characteristics

4.2.4.1 Zone Identification

, 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. **[**SPPRAMSS-10420 **]**

4.2.4.2 Accountable Organisations

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

4.2.4.3 Logical and Physical Boundary

, SP-SEC-Comp-4.2.4.3-1 - The physical boundary of the Zone-SC in context of this specification is the encasing of the Secure Component.
Note: Further physical boundaries may exists in the environment (rack, cabinet, room) or inside the Secure Component (composed devices, e.g. host with virtual machine). **[**SPPRAMSS-10419 **]**

, 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. **[**SPPRAMSS-11977 **]**

4.2.4.4 Safety Designation

, 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. **[**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).
Note: safety-related standards describing safety levels are EN 50716 and EN 50126 **[**SPPRAMSS-10421 **]**

4.2.4.5 Logical and Physical Access Points

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

, 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

[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. **[**SPPRAMSS-12039 **]**

4.2.4.6 Risk of Zone Assets

📄**, SP-SEC-Comp-4.2.4.6-1 -** The main risks for the asset in the Zone-SC (the Secure Component) is a compromise of the following protection objectives:

1. Integrity: can lead to loss of control, loss of safety, loss of essential functions
2. Availability: can lead to loss of control, loss of operation
3. Confidentiality: can lead to attacks on integrity and availability when confidential key material is extracted (impersonating attack)

Note: a detailed list of threats is described in [SP-SEC-ThreatCat]. **[**SPPRAMSS-10398 **]**

4.2.5 Operating Environment Assumptions

📄**, 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 SP-SEC-PGRM-6.2 - Physical Access Control. **[**SPPRAMSS-9617 **]**

📄**, SP-SEC-Comp-4.2.5-2 -** It is assumed that a Secure Component has connectivity to the shared cybersecurity services as defined in [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) **[**SPPRAMSS-9612 **]**

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

📄**, 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 [SP-SEC-DocTempl] . **[**SPPRAMSS-10439 **]**

4.2.6 Threat Environment

📄**, 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. **[**SPPRAMSS-9615 **]**

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

4.2.7 Threat and Risk Analysis Result

📄**, SP-SEC-Comp-4.2.7-1 -** The initial risk analysis is documented in [SP-SEC-ThreatAna]
[SPPRAMSS-9609 **]**

5 List of Detailed Security Requirements

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,...)

5.1 General

, **SP-SEC-Comp-5.1-1 -** The Secure Component shall be developed according to [IEC 62443-4-1:2018] (maturity level 3 at minimum).

Note: from table 1 - maturity levels of IEC 62443-4-1: maturity level 3 is achieved when a level 2 process has been practiced at least for one product (with required evidence).
Note: This requirement is not applicable for 3rd party or open source software integrated in the Secure Component. Security for these components is handled SP-SEC-PrgmReq Ch 13.2 Supply Chain Security) **[**Generic , SPPRAMSS-2495 **]**

, **SP-SEC-Comp-5.1-2 -** The Secure Component shall use for implementation of security functionality proven or mature security libraries and security hardware.

Note: proven/mature security libraries are widely and internationally used programming libraries. An example of a such security library is openSSL and operating system functions for obtaining random numbers. Using proven/mature security libraries limits implementation errors and risks of side-channel attacks, as well as purging of key material.
Proven/mature security hardware refers to widely recognized and internationally used hardware components specifically designed for security purposes. Examples of standard security hardware include cryptographic modules certified under FIPS 140-2, tamper-resistant secure elements, and hardware security modules (HSMs),Trusted Platform Module (TPM) chips and CPUs with Trusted Execution Environments (TEE). **[**Generic , SPPRAMSS-9632 **]**

5.2 Device Hardware

5.2.1 Real Time Clock

, **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. **[**Generic , SPPRAMSS-3873 **]**

, **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. **[**Generic , SPPRAMSS-7462 **]**

5.2.2 Random Number Generation

, **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 [RFC 4086]. **[**SPPRAMSS-9665 **]**

5.2.3 Hardware Trust Anchor

, 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. **[**Generic , SPPRAMSS-2941 **]**

, 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). **[**Generic , SPPRAMSS-3099 **]**

5.2.4 Hardware-related Firmware Update

, 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. **[**Generic , SPPRAMSS-3102 **]**

5.2.5 Secure Boot

, SP-SEC-Comp-5.2.5-1 - The Secure Component shall use the Secure Boot functions defined by the used chipset manufacturer. **[**Generic , SPPRAMSS-3105 **]**

, SP-SEC-Comp-5.2.5-2 - The Secure Component shall verify the authenticity of the firmware, bootloader, and operating system using trusted public keys or certificate chains managed by the manufacturer. **[**Generic , SPPRAMSS-6577 **]**

, SP-SEC-Comp-5.2.5-3 - If a secure boot verification fails, the Secure Component should provide a visible or audible indication.
Note: the visual or audible indication of an integrity check failure is recommended, as the Secure Component cannot securely log errors before successful start-up of the operating system. Examples could be a LED indication or audible notification. For COTS devices as PCs, laptops and servers, refer to manufacturer handbook for indications of a integrity failure during secure boot **[**SPPRAMSS-3429 **]**

, 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. **[**Generic , SPPRAMSS-2473 **]**

, 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. **[**Generic , SPPRAMSS-3729 **]**

, 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. **[**Generic , SPPRAMSS-4911 **]**

5.2.6 Electronic Tamper Detection

, **SP-SEC-Comp-5.2.6-1 -** When powered, the Secure Component or its installation encasing shall provide a tamper detection mechanism which detects the opening of the physical encasing.
Note: A typical installation encasing is a cabinet. **[**Generic , SPPRAMSS-3111 **]**

, **SP-SEC-Comp-5.2.6-2 -** If tampering is detected and the Secure Component implements tamper detection, the Secure Component shall provide notification of the detection to the SSI-LOG service. **[**Generic , SPPRAMSS-3110 **]**

, **SP-SEC-Comp-5.2.6-3 -** If tampering is detected and tamper detection is delegated to the operational environment, the operational environment shall provide notification of the detection for all Secure Components in that operational environment to the SSI-LOG service. **[**Generic , SPPRAMSS-15567 **]**

5.2.7 Physical Security Seal

, **SP-SEC-Comp-5.2.7-1 -** The supplier shall provide a security seal on the Secure Component or its installation encasing.
Note: A typical installation encasing is a cabinet. **[**Generic , SPPRAMSS-2994 **]**

, **SP-SEC-Comp-5.2.7-2 -** The security seal shall contain a number unique to the supplier. **[**Generic , SPPRAMSS-2998 **]**

, **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.
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 , SPPRAMSS-2634 **]**

, **SP-SEC-Comp-5.2.7-4 -** The seals shall be designed to break in case of standard attacks using heat or solvents. **[**Generic , SPPRAMSS-2637 **]**

5.2.8 Physical Identification

, **SP-SEC-Comp-5.2.8-1 -** The Secure Component shall bear a type, batch or serial number on its enclosure. **[**Generic , SPPRAMSS-13008 **]**

5.2.9 Physical Diagnostic Interfaces

, **SP-SEC-Comp-5.2.9-1 -** If physical diagnostic and test interfaces are accessible without opening the protected enclosure, the Secure Component shall disable physical factory diagnostic and test interfaces during manufacturing or commissioning. **[**Generic , SPPRAMSS-6695 **]**

5.2.10 Crypto Agility

, SP-SEC-Comp-5.2.10-1 - The Secure Component should be designed with crypto agility in mind. It is envisioned, 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. **[**SPPRAMSS-10110 **]**

5.3 Device Software

5.3.1 Process Runtime Integrity Check

, SP-SEC-Comp-5.3.1-1 - The Secure Component shall only start a software process if it passes the runtime integrity check.

Note: This protects against execution of unauthorised software. Typical solutions are a process allowlist or anomaly detection. An allowlist typically contains the hashes of the authorised executable binaries. **[**Generic , SPPRAMSS-3015 **]**

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

Note: if the process runtime-integrity check is realised using an process allowlist, this could be part of the firmware and therefore is part of the secure boot process. If the allowlist is outside of the secure boot process (e.g. on a configuration partition), a possible solution is the signing of the allowlist with the certificate of the software manufacturer. **[**Generic , SPPRAMSS-3720 **]**

5.3.2 Persistent Data Integrity

, 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. **[**Generic , SPPRAMSS-2471 **]**

, 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. **[**Generic , SPPRAMSS-2488 **]**

, 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.

Note: If personal identifiable information or financial data is recorded, as of GDPR also confidentiality needs to be considered **[**Generic , SPPRAMSS-2493 **]**

5.3.3 Persistent Data Confidentiality

, **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. **[**Generic , SPPRAMSS-3013 **]**

5.3.4 Input Validation

, **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. **[**Generic , SPPRAMSS-3023 **]**

5.3.5 Deterministic Output

, **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. **[**Generic , SPPRAMSS-3022 **]**

5.3.6 Hardening

, **SP-SEC-Comp-5.3.6-1 -** The Secure Component shall enable only required and documented functions and services and their corresponding exposed ports and protocols.

Note: Examples for possible unused functions and services are email, voice over IP, instant messaging, and file transfer protocol (FTP). This requirement can be verfied by external port scans (no difference between documented required ports and detected ports). When using standard OS and applications, OS and application hardenening can be an essential measure to fulfill this requirement. Hardening can be demonstrated by a relevant **[CIS benchmark]**, achieving compliance to at least Level 1 or in accordance with a comparable benchmark and compliance level. **[**Generic , SPPRAMSS-3779 **]**

5.3.7 Time Synchronisation

, **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). **[**Generic , SPPRAMSS-2301 **]**

, **SP-SEC-Comp-5.3.7-2 -** The Secure Component shall update its internal real-time clock with the synchronized time received via interface SSI-STS (refer to SP-SEC-ServSpec Ch 4 - STS: Secure Time Synchronisation). **[**Generic , SPPRAMSS-7524 **]**

5.4 Network Capabilities

5.4.1 VLAN Support

, **SP-SEC-Comp-5.4.1-1 -** VLAN tagging is optional. The referencing specification (e.g. EULYNX, future TSI) will define if VLAN tagging shall be used. **[**SPPRAMSS-15505 **]**

, **SP-SEC-Comp-5.4.1-2 -** The Secure Component can 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 **]**

, **SP-SEC-Comp-5.4.1-3 -** The Secure Component can be capable to bind each communicating process to configured interface(s) corresponding to a specific VLAN. **[**SPPRAMSS-7526 **]**

, **SP-SEC-Comp-5.4.1-4 -** The Secure Component can be capable to separate at least maintenance (e.g. SMI), diagnostic (e.g. SDI), security (e.g. SSI) and operational data (e.g. SCI) to specific VLANs.

Note: There could be additional VLANS for example for further segmentation of SCI (different SIL level, different SSI-XXX), on-board specific VLANs. This further segmentation can be configured via the component configuration. **[**SPPRAMSS-7528 **]**

5.4.2 Host-based Firewall

, **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). **[**Generic , SPPRAMSS-3822 **]**

, **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. **[**Generic , SPPRAMSS-3821 **]**

, **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. **[**Generic , SPPRAMSS-2555 **]**

, **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. **[**Generic , SPPRAMSS-7529 **]**

5.4.3 Network Access Control

, **SP-SEC-Comp-5.4.3-1 -** The Secure Component shall support to authenticate to the network using the SSI-NAC interface (refer to SP-SEC-ServSpec Ch 8 - NAC: Network Access Control). **[**Generic , SPPRAMSS-2315 **]**

, **SP-SEC-Comp-5.4.3-2 -** The Secure Component shall use the Operator Device Certificate (ODC) as specified in SP-SEC-ServSpec Ch 13.1.2-1 - Operator Device Certificate for authentication towards the Network Authentication Server. **[**Generic , SPPRAMSS-4892 **]**

, **SP-SEC-Comp-5.4.3-3 -** If no Operator Device Certificate (ODC) is available, the Secure component shall use the Manufacturer Device Certificate (MDC) as specified in SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate 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) **[**Generic , SPPRAMSS-4891 **]**

5.4.4 Denial of Service Resilience

, **SP-SEC-Comp-5.4.4-1 -** The Secure Component shall limit use of system resources by security functions to protect against resource exhaustion.

Note: This can be tested by monitoring system resources as CPU utilization, volatile memory, persistence memory and network utilization during normal and stress situations over an extended period of time. The test should show that resource utilization stays in the specified limits. **[**Generic , SPPRAMSS-9633 **]**

, **SP-SEC-Comp-5.4.4-2 -** After a Denial of Service (DoS) event (e.g. saturation / high load of the network interface), the Secure Component shall operate normally.

Note: recommended test time for network saturation is at least one minute, recommended time to check for normal operation after network saturation is 30 seconds.

This supports maintaining essential functions in a degraded mode as the result of a DoS event, together with SP-SEC-Comp-5.4.4-3 and SP-SEC-Comp-5.4.4-1 **[**Generic , SPPRAMSS-3781 **]**

, **SP-SEC-Comp-5.4.4-3 -** The Secure Component shall provide the capability to only allow a configurable maximum number of concurrent sessions per interface for any given user (human, or technical user). **[**Generic , SPPRAMSS-2630 **]**

5.4.5 Minimisation of Data

, **SP-SEC-Comp-5.4.5-1 -** The Secure Component shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the Secure Component (‘data minimisation’). **[**Generic , SPPRAMSS-13014 **]**

5.5 Identification, Authentication & Authorisation

5.5.1 Identification, Authentication and Authorisation of Standard Communication Interfaces

, **SP-SEC-Comp-5.5.1-1 -** If the Secure Component uses the standard communication protocols defined in [SP-SEC-CommSpec], the Secure Component shall implement the requirements from the [SP-SEC-CommSpec]. **[**Generic , SPPRAMSS-6676 **]**

, **SP-SEC-Comp-5.5.1-2 -** The Secure Component shall implement the interfaces defined in [SP-SEC-ServSpec].

Note1: 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 7 of [SP-SEC-CommSpec]

Note2: Usage of SSI between the SCS is not mandatory, but recommended. **[**Generic , SPPRAMSS-6675 **]**

5.5.2 Public Key Certificates

, SP-SEC-Comp-5.5.2-1 - The Secure Component shall implement the interface SP-SEC-ServSpec Ch 6 - Public Key Infrastructure to request certificates. **[**Generic , SPPRAMSS-2324 **]**

, SP-SEC-Comp-5.5.2-2 - The Secure Component shall generate a new individual key pair for every requested and renewed certificate. **[**Generic , SPPRAMSS-4180 **]**

, SP-SEC-Comp-5.5.2-3 - The Secure Component shall generate keys on the Secure Component itself. **[**Generic , SPPRAMSS-2509 **]**

, SP-SEC-Comp-5.5.2-4 - The Secure Component shall implement the interface SP-SEC-ServSpec Ch 5 - PKI: Public Key Infrastructure to renew a certificate. **[**Generic , SPPRAMSS-2322 **]**

, SP-SEC-Comp-5.5.2-5 - The Secure Component shall automatically request the renewal of its certificates a configurable number of days in advance to the certificate's expiration date.

Note: after rekeying a certificate, it is recommended to not revoke the old certificate to keep CRLs manageable. **[**Generic , SPPRAMSS-2335 **]**

, SP-SEC-Comp-5.5.2-6 - If a certificate is renewed, the Secure Component shall use the renewed certificate for subsequent connection establishments.

Note: This means that active connections continue using the original certificate until that certificate is revoked **[**Generic , SPPRAMSS-16307 **]**

, SP-SEC-Comp-5.5.2-7 - The Secure Component shall be able to trust a list of at least 10 certificate authorities.

Note: more trusted certificate authorities may be needed depending on the intended operation of a Secure Component, related to the number of entities (e.g. IMs or RUs) taking part in the operation. **[**Generic , SPPRAMSS-2428 **]**

, SP-SEC-Comp-5.5.2-8 - The Secure Component shall update its CRLs via the SSI-PKI interface. **[**Generic , SPPRAMSS-2437 **]**

, SP-SEC-Comp-5.5.2-9 - The Secure Component shall update its CRLs as defined in RFC 5280 chapter 6.3.3 or by using externally configured CRL distribution points.

Note1: a diagnostic method is also available to trigger a CRL update when required. See SP-SEC-Serv-12.2-1

Note2: CRL Distribution Points hosted by manufacturers can be mapped to internal CRL Distribution Points hosted by operators using Split-DNS (see SP-SEC-ServSpec Ch 13.7 - DNS SP-SEC-ServSpec Chapter 13 - DNS)

[Generic , SPPRAMSS-12353 **]**

, SP-SEC-Comp-5.5.2-10 - 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. **[**Generic , SPPRAMSS-8039 **]**

, SP-SEC-Comp-5.5.2-11 - The Secure Component shall support certificates defined in SP-SEC-ServSpec Ch 14.1 - Certificate Profiles. **[**Generic , SPPRAMSS-2435 **]**

, SP-SEC-Comp-5.5.2-12 - If more than one network interface is used for safety communication, the Secure Component shall use a dedicated OSCC for each network interface.
Note: this ensures that if the communication certificate of one network interface is renewed, the connection over the other network interface maintains its independency. **[**Generic , SPPRAMSS-16351 **]**

5.5.3 PKI Certificate Validation

, SP-SEC-Comp-5.5.3-1 - The Secure Component shall check if the certificate signature is valid. **[**Generic , SPPRAMSS-6679 **]**

, SP-SEC-Comp-5.5.3-2 - The Secure Component shall validate the certificate's trust chain up to a trusted certificate authority. **[**Generic , SPPRAMSS-2432 **]**

, SP-SEC-Comp-5.5.3-3 - The Secure Component shall check if the certificate is not revoked using CRLs. **[**Generic , SPPRAMSS-2431 **]**

, SP-SEC-Comp-5.5.3-4 - 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. **[**Generic , SPPRAMSS-7579 **]**

, SP-SEC-Comp-5.5.3-5 - The Secure Component shall map the authenticated identity of a certificate to a user (human or technical user). **[**Generic , SPPRAMSS-6660 **]**

, SP-SEC-Comp-5.5.3-6 - The Secure Component shall validate and enforce the extended key usage according to the definition in SP-SEC-ServSpec Ch 14.1 Certificate Profiles. **[**Generic , SPPRAMSS-9989 **]**

, SP-SEC-Comp-5.5.3-7 - If the Secure Component cannot validate certificates because of a missing secure time source (e.g. during initial commissioning), the Secure Component shall use a fallback time source.
Note: The fallback time can for example be calculated using the following (possibly non-secure) time sources: NTP, last shutdown time, real-time clock of the device. **[**Generic , SPPRAMSS-7967 **]**

5.5.4 Commissioning Procedure

For SCS implementations, the Commissioning Procedure is not mandatory but recommended.
Note: For trackside SCS, the PKI Commissioning Procedure is recommended. For onboard SCS or deployments requiring automated lifecycle management, the PKI Commissioning Procedure may become mandatory in future versions of this specification

, SP-SEC-Comp-5.5.4-1 - The Secure Component shall have the capability to accept initial device configuration signed by manufacturer or operator.
Note: the initial device configuration is intended for the commissioning phase, it includes PKI configuration (including information which certificates a Secure Component needs to request), CRLs and operator trust anchor (see SP-SEC-Comp-5.5.4-6)
[Generic , SPPRAMSS-16308 **]**

, SP-SEC-Comp-5.5.4-2 - The Secure Component shall contain the following configuration items before starting the commissioning process :

- IP-Address or FQDN of SCS-PKI

- IP-Address or FQDN of SCS-STS
- IP-Address or FQDN of SCS-IAM
- Operator Trust Anchor
- Identifiers required for operator certificate requests (e.g. EULYNX identifier)

Note: For initial provisioning of software and configuration initially the address of the update/config server (e.g. MDM) is required. Configuration items are defined in SP-SEC-Comp-6.2-2 Configuration items **[**Generic , SPPRAMSS-4960 **]**

, **SP-SEC-Comp-5.5.4-3 -** The Secure Component shall skip the verification of the server certificate of the SCS-NAC.
Note: this means that CRLs are not required to perform network authentication **[**Generic , SPPRAMSS-16280 **]**

, **SP-SEC-Comp-5.5.4-4 -** The Secure Component shall initially synchronise time using SCS-STS via NTP after gaining network access.
Note: Validation of certificates using fallback time is defined in SP-SEC-Comm - Certificate Validation **[**Generic , SPPRAMSS-16282 **]**

, **SP-SEC-Comp-5.5.4-5 -** The Secure Component shall be equipped with a Manufacturer Device Certificate (MDC) which includes the unique serial number of the Secure Component as described in SP-SEC-ServSpec Ch 13.1.1-1 - Manufacturer Device Certificate (MDC) profile. **[**Generic , SPPRAMSS-16281 **]**

, **SP-SEC-Comp-5.5.4-6 -** The MDC including its certifiate chain required to validate the certificate shall be installed on the Secure Component before commissioning (see also SP-SEC-CompSpec Ch 5.5.5-1).
Note: the key pair for the MDC is generated on the Secure Component (see SP-SEC-Comp-5.5.2-3) **[**Generic , SPPRAMSS-7583 **]**

, **SP-SEC-Comp-5.5.4-7 -** The Secure Component shall have the capability to install and remove Operator Root CA Certificates (ORCACs) that are defined in a configuration file signed by the Manufacturer Trust Anchor Signer Certificate (MTASC). **[**Generic , SPPRAMSS-7597 **]**

, **SP-SEC-Comp-5.5.4-8 -** The Secure Component shall have the capability to install and remove Operator Root CA Certificates (ORCACs) that are defined in a configuration file signed by the Operator Trust Anchor Signer Certificate (OTASC). **[**Generic , SPPRAMSS-15903 **]**

, **SP-SEC-Comp-5.5.4-9 -** The Secure Component shall only accept an Operator Root CA Certificate (ORCAC) signed by the Manufacturer Trust Anchor Signer Certificate (MTASC) if it has no ORCAC yet. **[**Generic , SPPRAMSS-15902 **]**

, **SP-SEC-Comp-5.5.4-10 -** The Secure Component shall request the Operator Device Certificate (ODC) via the SSI-PKI interface using the Manufacturer Device Certificate (MDC) for message protection. **[**Generic , SPPRAMSS-4961 **]**

, **SP-SEC-Comp-5.5.4-11 -** The Secure Component shall request all other operator certificates (ONCC, OSCC, OUC, OCSC, see SP-SEC-ServSpec Ch 5.1.3 - Use Case: Updating Operator Certificates) via the SSI-PKI interface using the Operator Device Certificate (ODC) for message protection. **[**Generic , SPPRAMSS-4962 **]**

, SP-SEC-Comp-5.5.4-12 - Overview of commissioning steps:

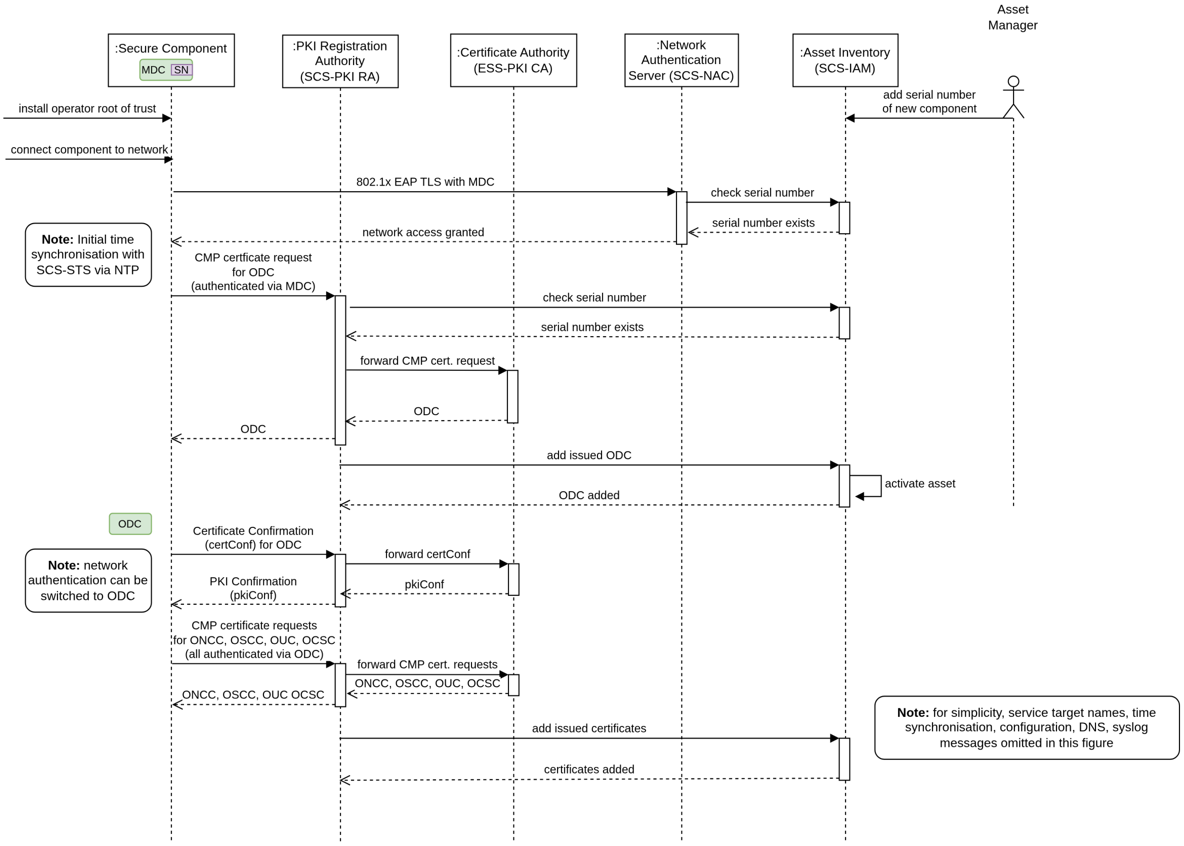

:Secure Component
MDC
SN
:PKI Registration Authority (SCS-PKI RA)
:Certificate Authority (ESS-PKI CA)
:Network Authentication Server (SCS-NAC)
:Asset Inventory (SCS-IAM)
Asset Manager
install operator root of trust
add serial number of new component
connect component to network
802.1x EAP TLS with MDC
check serial number
serial number exists
network access granted
Note: Initial time synchronisation with SCS-STS via NTP
CMP certficate request for ODC (authenticated via MDC)
check serial number
serial number exists
forward CMP cert. request
ODC
ODC
add issued ODC
activate asset
ODC added
ODC
Certificate Confirmation (certConf) for ODC
forward certConf
Note: network authentication can be switched to ODC
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
add issued certificates
Note: for simplicity, service target names, time synchronisation, configuration, DNS, syslog messages omitted in this figure
certificates added

Figure 4 Overview of commissioning steps

[SPPRAMSS-11556 **]**

, SP-SEC-Comp-5.5.4-13 - For validation and testing purposes there might be additional certificate types used. **[**SPPRAMSS-7581 **]**

, SP-SEC-Comp-5.5.4-14 - Additional checks between RA and asset manager are optional. The operator may define metadata to be checked. **[**SPPRAMSS-9941 **]**

, SP-SEC-Comp-5.5.4-15 - Usage of different networks for commissioning is optional and not depicted in the drawing. **[**SPPRAMSS-9991 **]**

, SP-SEC-Comp-5.5.4-16 - After the commissioning process the following steps can be performed:

- Secure time synchronisation with SCS-STS (via NTS)
- Fetch software and configuration via OPC-UA from the update/config server (e.g. MDM) (including concurrent request to the SCS-IAM for permission management)
- Establish connections to further SCS based on the provided configuration data (e.g. SCS-LOG

[SPPRAMSS-16283 **]**

5.5.5 Trust Anchor Installation

, SP-SEC-Comp-5.5.5-1 - The Secure Component shall have the capability to install trusted certificates in the trust store via the mechanism described in Chapter SP-SEC-CompSpec Ch 5.6.1 - Software Update. **[**Generic , SPPRAMSS-4967 **]**

5.6 Software Update, Backup and Restore

For SCS implementations, the Software Update, Backup and Restore requirements using SCS and MDM are not mandatory but recommended.

Note: For SCS implementations, backup and restore mechanisms are still required, but can be implemented using alternative mechanisms. These alternative mechanisms should align with SP-SEC-Pgrm Chapter 12.3 Backup and Restore to ensure equivalent security and auditability.

5.6.1 Software Update

, SP-SEC-Comp-5.6.1-1 - The Secure Component shall support the update of software and configuration via the interface [I-STD-MAINTENANCE - SMI] .

Note 1: when updating non-safety related software, typically also the process allowlist has to be updated.

Note 2: this supports together with the backup and restore functionality (chapter 5.6.3) the recovery and reconstitution to a known secure state after a disruption or failure. **[**Generic , SPPRAMSS-2497 **]**

, SP-SEC-Comp-5.6.1-2 - The Secure Component 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 , SPPRAMSS-2503 **]**

, 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. **[**Generic , SPPRAMSS-2982 **]**

, SP-SEC-Comp-5.6.1-4 - The Secure Component shall reject update packages without a valid signature. **[**Generic , SPPRAMSS-2984 **]**

5.6.2 Update Package

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.

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

[Generic , SPPRAMSS-4028 **]**

, SP-SEC-Comp-5.6.2-2 - The update package shall use SHA-512 hash algorithm for the integrity protection. **[**Generic , SPPRAMSS-2498 **]**

, 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. **[**Generic , SPPRAMSS-2989 **]**

5.6.3 Backup and Restore

, SP-SEC-Comp-5.6.3-1 - If operational data is not part of the configuration data from [I-STD-MAINTENANCE - SMI] interface, the Secure Component shall backup operational data which is relevant for its operational availability via SSI-BKP SP-SEC-Serv - Ch. 11 - BKP: Backup and Restore
Note 1: Backups are intended for operational data that is relevant for operational availability (e.g. changes in databases), but is not part of the configuration (e.g. obtained via I-STD-MAINTENANCE (SMI)). Most rail automation devices receive all data required for operational data via I-STD-MAINTENANCE and do not need the interface SSI-BKP
Note 2: Backups are triggered remotely via SSI-BKP, additionally the Secure Component has also the option to trigger a backup creation locally , e.g. based on time or change events. **[**Generic , SPPRAMSS-3078 **]**

, SP-SEC-Comp-5.6.3-2 - If the Secure Component backups operational data , the Secure Component shall be capable of restoring operational data via SSI-BKP SP-SEC-ServSpec Ch 11 - BKP: Backup and Restore **[**Generic , SPPRAMSS-6750 **]**

, SP-SEC-Comp-5.6.3-3 - If the Secure Component backups operational data, the Secure Component shall be capable of verifying the authenticity and integrity of backup data received via SSI-BKP SP-SEC-ServSpec Ch 11 - BKP: Backup and Restore **[**Generic , SPPRAMSS-6749 **]**

5.7 Logging and Diagnostics

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.

5.7.1 Security Logging

, 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).

Note: more detail of log events is described in chapter SP-SEC-ServSpec Ch 9.1 - Log Message Format **[**Generic , SPPRAMSS-2581 **]**

, SP-SEC-Comp-5.7.1-2 - The Secure Component shall send the logging events via SSI-LOG SP-SEC-ServSpec Ch 9 - LOG: Security Logging .

Note: this ensures encryption of the log messages and ensures that no information is provided that can be exploited by adversaries to attack the system. **[**Generic , SPPRAMSS-2580 **]**

, **SP-SEC-Comp-5.7.1-3 -** The Secure Component shall provide the capability to send logging data to at least four configurable log collector destinations. **[**Generic , SPPRAMSS-4407 **]**

, **SP-SEC-Comp-5.7.1-4 -** The Secure Component shall send log messages complying to the log message format defined in SP-SEC-ServSpec Ch 9.1 - Log Message Format

Note: This ensures that the log messages contain the following data:
a) timestamp (synchronized);
b) source (originating device, software process or human user account);
c) category;
d) type;
e) event ID; and
f) event result **[**Generic , SPPRAMSS-2588 **]**

, **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 SP-SEC-Serv Ch 12.3 - Log Maintenance . The untransferred logs are assumed to be accessible until a restart / reboot. **[**Generic , SPPRAMSS-2598 **]**

, **SP-SEC-Comp-5.7.1-6 -** The Secure Component implementing a Log Server (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. **[**Generic , SPPRAMSS-2597 **]**

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

, **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. **[**Generic , SPPRAMSS-3070 **]**

, **SP-SEC-Comp-5.7.1-9 -** 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. **[**SPPRAMSS-12067 **]**

5.7.2 Security Maintenance and Diagnostics

, **SP-SEC-Comp-5.7.2-1 -** The Secure Component supports the verification of the intended operation of security functions by the diagnostic values and maintenance methods in this chapter.

Note: For SCS implementations, the functionality in the table below may be provided by existing secure administration interfaces instead of SSI-MNT.

Security Function	Verification	Verification time
Process Allowlisting	maintenance call 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 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
Identification and Authentication	any call to the maintenance interface involves user identification and authentication, testable using different users with different permissions	during normal operation
User Authorization	any call to the maintenance interface involves user authorization, testable using different users with different permissions	during normal operation
Random number generation	verification of using OS standard implementation for random number generation, check randomness for seeds after boot-up (esp. for components without a battery-buffered clock), check of entropy of random number generation	during product development
Electronic tamper detection	check detection when opening the encasing	during product development
Input validation	Fuzz testing	

Security Function	Verification	Verification time
		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

[SPPRAMSS-3010 **]**

6 Manufacturing, Configuration, Documentation

6.1 Secure Component Manufacturing

, **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. **[**Generic , SPPRAMSS-2308 **]**

6.2 Secure Component Configuration

This chapter lists the configuration items of a Secure Component. These configuration items can be set by the owner of the Secure Component. The role-based access control is configured in the SCS-IAM. The configuration items regarding password strength are included to comply with IEC 62443-4-2 CR 1.7.

Note: For SCS implementations, configuration items may be managed via existing secure administration interfaces instead of SMI.

, **SP-SEC-Comp-6.2-1 -** The Secure Component shall support the SMI interface for updating the security configuration. **[**Generic , SPPRAMSS-3086 **]**

, **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 address)
- IP addresses / FQDN to all shared cybersecurity services instances, support for at least four instances per service for high availability
- binding of communication processes to VLANs / interfaces
- time (days or hours) before expiration date to start certificate renewal
- time period of inactivity of a human user session
- action after time period of inactivity by human user (lock session or terminate session)

[Generic , SPPRAMSS-6672 **]**

, **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. **[**Generic , SPPRAMSS-6886 **]**

, **SP-SEC-Comp-6.2-4 -** If the Secure Component supports local password-based authentication, the Secure Component shall provide following configuration items:

- password rules (minimum length, variety of character types)
- number of generations before reusing a password
- minimum and maximum password lifetime
- number of consecutive invalid access attempts
- time period to deny access when the limit of consecutive invalid login attempts has been reached
- number of days before password expiration to prompt the human user to change their password

Note 1: The Secure Component implementing the SSI-UAS service should support password-based authentication and the password configuration items.

Note 2: Secure Components using user authentication via the SSI-UAS interface do not need to support password-based authentication or password configuration items.
Note 3: Common security practices recommend to only change passwords when there is an indication of compromise. Therefore, the maximum password lifetime should be set to infinite (e.g. a long time in the future). **[**Generic , SPPRAMSS-6661 **]**

6.3 Component Documentation

, SP-SEC-Comp-6.3-1 - The Secure Component shall include the information set out in the [SP-SEC-DocTempl] - Product Documentation Template in a document in a file format defined by an openly published specification accompanying the product.
Note: Such a file format may be for example PDF-A, Office Open XML, Drawing Interchange Format, Scalable Vector Graphics (SVG). **[**Generic , SPPRAMSS-6894 **]**

, 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. **[**Generic , SPPRAMSS-10305 **]**

, SP-SEC-Comp-6.3-3 - The manufacturer shall update continuously the Secure Component technical documentation, where appropriate, for at least during the support period. **[**Generic , SPPRAMSS-6884 **]**

7 Requirements for specific component types

7.1 COTS Network Components

, **SP-SEC-Comp-7.1-1 -** "This section contains the requirements mandatory for network components as part of the EU-Rail SP Security Scope (see SP-Sec-Arch document).

Note 1: Network components are only affected by requirements defined in this chapter.
Note 2: Network components are e.g. switches, routers, gateways and, firewalls. **[**SPPRAMSS-7694 **]**

7.1.1 Network Component Requirements

, **SP-SEC-Comp-7.1.1-1 -** The Network Component acting as a SCS-NAC Authenticator shall support IEEE 802.1x EAP TLS network authentication.
Note: IEEE 802.1x EAP TLS might also be required for trunk ports **[**Network , SPPRAMSS-10444 **]**

, **SP-SEC-Comp-7.1.1-2 -** The Network Component acting as a SCS-NAC Authenticator shall support the RFC 2865 RADIUS protocol for network authentication. **[**Network , SPPRAMSS-10446 **]**

, **SP-SEC-Comp-7.1.1-3 -** The Network Component shall support IEEE 802.1q VLAN tagging. **[**Network , SPPRAMSS-10445 **]**

, **SP-SEC-Comp-7.1.1-4 -** The Network Component shall support IEEE 802.1q priority code points, also referred as IEEE 801.1p. **[**Network , SPPRAMSS-10448 **]**

, **SP-SEC-Comp-7.1.1-5 -** 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. **[**Network , SPPRAMSS-10447 **]**

, **SP-SEC-Comp-7.1.1-6 -** The Network Component shall support sending logs and alarms via syslog (RFC 5424), preferable using Syslog over TLS (RFC 5425). **[**Network , SPPRAMSS-2602 **]**

, **SP-SEC-Comp-7.1.1-7 -** The Network Component shall support SNMPv3 (RFC 3410). **[**Network , SPPRAMSS-4392 **]**

, **SP-SEC-Comp-7.1.1-8 -** The Network Component should support detailed flow information forwarding to an analysis system (e.g. RFC 3954 NetFlow, RFC 3176 SFlow) **[**Network , SPPRAMSS-3834 **]**

, **SP-SEC-Comp-7.1.1-9 -** The Network Component shall support configuring a separate physical management port. **[**Network , SPPRAMSS-2627 **]**

, **SP-SEC-Comp-7.1.1-10 -** The Network Component shall support authentication on all enabled management network interfaces. **[**Network , SPPRAMSS-2524 **]**

, **SP-SEC-Comp-7.1.1-11 -** The Network Component shall support integrity and encryption protection for the protocols used for the enabled management network interfaces. **[**Network , SPPRAMSS-6764 **]**

7.1.2 Access from Untrusted Networks

, SP-SEC-Comp-7.1.2-1 - If the Network Component provides access from untrusted networks, the Network Component shall control and monitor the access. **[**Network , SPPRAMSS-6668 **]**

, SP-SEC-Comp-7.1.2-2 - If the Network Component provides access from untrusted networks, the Network Component shall be capable of denying access via untrusted networks unless explicitly approved by an assigned role. **[**Network , SPPRAMSS-6669 **]**

7.1.3 Network-based Firewall

, 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). **[**Network , SPPRAMSS-2542 **]**

, 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. **[**Network , SPPRAMSS-3831 **]**

, SP-SEC-Comp-7.1.3-3 - The Network Component at a zone boundary implementing a firewall shall be capable of enabling an island mode.

Note: island mode is defined as blocking or disabling interfaces to another network zone (e.g. from signalling network to back-office or enterprise network) **[**Network , SPPRAMSS-3059 **]**

, SP-SEC-Comp-7.1.3-4 - The Network Component at a zone boundary implementing a firewall shall automatically block connections (fail close) during a failure of the network filter mechanisms. **[**Network , SPPRAMSS-3058 **]**

7.1.4 Wireless Access Management

, 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. **[**Wireless , SPPRAMSS-6600 **]**

7.2 Components with HMIs

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

, 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. **[**HMI, SPPRAMSS-2292 **]**

, SP-SEC-Comp-7.2-3 - If a Secure Components implementing a Shared Cybersecurity Service with a human-machine interface (e.g. IAM, software update system) allows high-risk operations, the Secure Components implementing a Shared Cybersecurity Service shall be capable to enforce the dual control principle.

Note. Examples for high-risk operations are: assign admin role, update security configuration or software. [HMI, SPPRAMSS-2972]

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

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

, **SP-SEC-Comp-7.2-6 -** If the Secure Component provides a human-machine interface, the Secure Component shall unlock the locked human-user sessions only after re-authentication of the human user.
Note: See also SP-SEC-Comp-7.2-7 for supervisor override in case of HMI controlling essential services. [HMI, SPPRAMSS-6693]

, **SP-SEC-Comp-7.2-7 -** If the Secure Component implements a human-machine interface which is needed to control an essential service, the Secure Component shall support a supervisor manual override for a configurable time or sequence of events. [HMI, SPPRAMSS-6670]

, **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, SPPRAMSS-13043]

, **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, SPPRAMSS-13044]

, **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]** [HMI, SPPRAMSS-13362]

, **SP-SEC-Comp-7.2-11 -** For a pyhsically protected location including multiple HMIs for a single user, this user may be authenticated by one method for all relevant HMIs.
Note: An example of such an environment is a driver cabin, where a train driver has access to multiple essential functions for train operation. [SPPRAMSS-16305]

7.3 Components using Password-based Authentication

, **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. e.g. it does not integrate into an user authentication service (SCS-UAS) password-based authentication.
Note: Chapter 6.2 lists all configuration items of a Secure Component. [SPPRAMSS-6654]

, SP-SEC-Comp-7.3-2 - If the Secure Component supports local password-based authentication and local user management, then Secure Component shall enforce configurable password strength (minimum length, variety of character types). **[**Generic , SPPRAMSS-6655 **]**

, SP-SEC-Comp-7.3-3 - If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall provide the capability to protect against any given human user account from reusing a password for a configurable number of generations. **[**Generic , SPPRAMSS-6658 **]**

, SP-SEC-Comp-7.3-4 - If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall provide the capability to enforce password minimum and maximum lifetime restrictions for all human users. **[**Generic , SPPRAMSS-6656 **]**

, SP-SEC-Comp-7.3-5 - If the Secure Component supports 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. **[**Generic , SPPRAMSS-6657 **]**

, SP-SEC-Comp-7.3-6 - If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall limit the number of consecutive invalid access attempts by any user (human or technical user). **[**Generic , SPPRAMSS-3885 **]**

, SP-SEC-Comp-7.3-7 - If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall deny access for a specific period of time when the limit of consecutive invalid attempts is reached. **[**Generic , SPPRAMSS-6664 **]**

, SP-SEC-Comp-7.3-8 - If the Secure Component supports local password-based authentication and local user management and user accounts can be locked (e.g. due consecutive invalid access attempts), then the Secure Component shall be capable to unlock a locked account by an administrator
[Generic , SPPRAMSS-6663 **]**

, SP-SEC-Comp-7.3-9 - If the Secure Component supports local password-based authentication and local user management, then the Secure Component shall obscure feedback of authentication information.

Note: In case of invalid username/password combination, the feedback is invalid username/password combination, not give hints that could help an attacker as "invalid user" or "invalid password", "password length insufficient". **[**Generic , SPPRAMSS-2966 **]**

7.4 Components using Symmetric Key-based Authentication

, 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. **[**Generic , SPPRAMSS-6665 **]**

, SP-SEC-Comp-7.4-2 - If symmetric key-based authentication is used due to interoperability requirements by TSI, the Secure Component shall protect the symmetric key-based authentication by another security layer conformant to chapter 4 of the Secure Communication Specification (SP-SEC-Comm Ch 3 - End-to-End Security Layer (TLS) .)

Note 1: the use of symmetric key-based authentication requires the distribution of the symmetric keys ensuring confidentiality. This can be done using PKI / asymmetric cryptography or a out-of-band transmission ensuring confidentiality.
Note 2: Symmetric key authentication does not conform to internationally recognized and proved security practices. The only reason to implement it, may be the TSI. In this case, the appropriate security will be provided by adding a second security layer which uses industry-wide accepted security mechanism. This is, for example, done with the ETCS communication with Subset-146 for symmetric cipher of Subset-137-2) **[**Generic , SPPRAMSS-6666 **]**

8 Residual risk

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])

8.1 Vulnerabilities in Secure Components or Network Components

🗎**, SP-SEC-Comp-8.1-1 -** Secure Components and Network Components are complex products composed of various hardware (chipsets, CPU,...) 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. **[**SPPRAMSS-13344 **]**

🗎**, SP-SEC-Comp-8.1-2 -** The 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. **[**SPPRAMSS-13342 **]**

🗎**, SP-SEC-Comp-8.1-3 -** Mitigation: Vulnerability Management (as defined in IEC 62443-4-1 DM1-DM6) and installation of security updates (see SP-SEC-PrgmReq Ch 8.1 Patch- and Vulnerability Management) **[**SPPRAMSS-13343 **]**

8.2 Compromise of Privileged accounts

🗎**, SP-SEC-Comp-8.2-1 -** 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. **[**SPPRAMSS-13348 **]**

🗎**, SP-SEC-Comp-8.2-2 -** 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. **[**SPPRAMSS-13347 **]**

🗎**, SP-SEC-Comp-8.2-3 -** Compromise of privileged accounts can be caused by social attacks (e.g. phishing, black mailing, quid pro quo, water-holing,...). **[**SPPRAMSS-13346 **]**

🗎**, SP-SEC-Comp-8.2-4 -** Mitigation: Training of security operators against account compromise and awareness of social attack threats (see SP-SEC-Prgm Ch 5.10 - Personell awareness training) **[**SPPRAMSS-13345 **]**

8.3 Supply Chain Attacks

🗎**, SP-SEC-Comp-8.3-1 -** Secure Component and Network Components can be compromised by introducing vulnerabilities in the supply chain. This can lead to undetected and undocumented exploitable vulnerabilities. **[**SPPRAMSS-13353 **]**

🗎**, SP-SEC-Comp-8.3-2 -** Several cases of supply chain attacks of hardware chipsets, open source software and 3rd party software has been recorded over the last years. **[**SPPRAMSS-13351 **]**

🗎**, SP-SEC-Comp-8.3-3 -** 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. **[**SPPRAMSS-13352 **]**

🗎 **, SP-SEC-Comp-8.3-4 -** 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. **[**SPPRAMSS-13349 **]**

🗎 **, SP-SEC-Comp-8.3-5 -** Mitigation: Anomaly detection systems (e.g. in NIDS) should be employed in environments of installed Secure Components to detect unexpected behaviour and communication attempts. **[**SPPRAMSS-13350 **]**

8.4 Security-related Application Conditions

🗎 **, SP-SEC-Comp-8.4-1 -** No additional application conditions have been identified beyond the requirements specified in the SP Cybersecurity requirements documents. **[**SPPRAMSS-13856 **]**