Taxonomy and References

Disclaimer

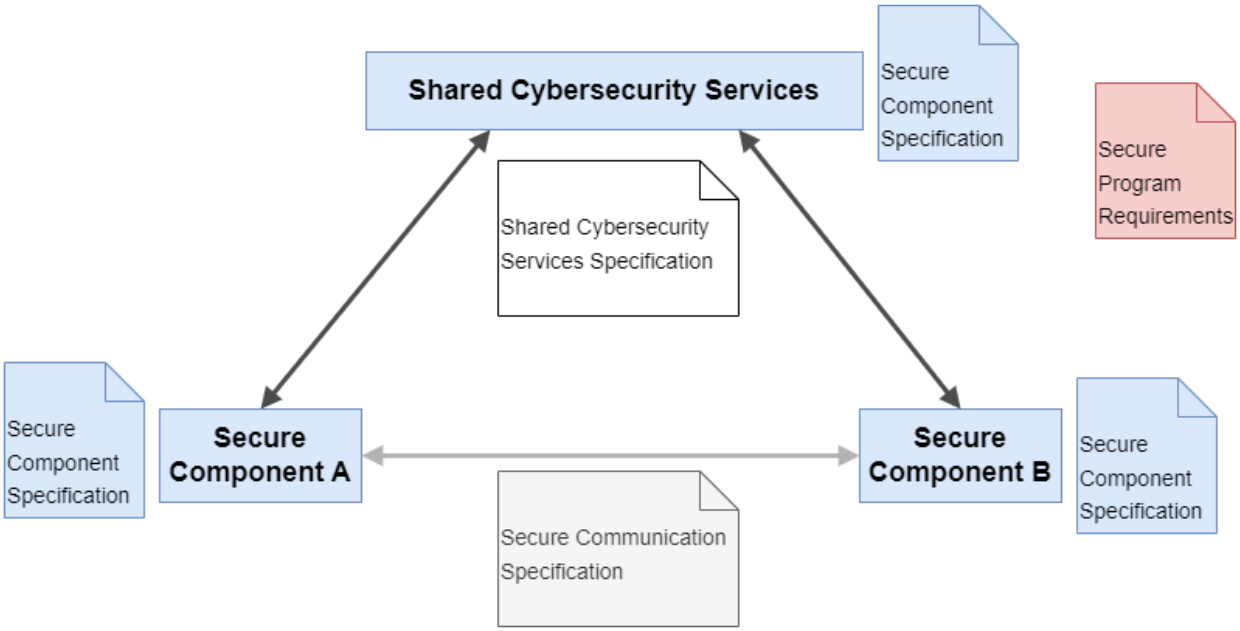
Maintenance

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

1 Table of Contents

2 Taxonomy

, SP-SEC-Tax-2-1 - Key terms and technical specs used in this document.



, SP-SEC-Tax-2-2 - TSI-requirements are directly derived from IEC 62443-3-3 as security requirements to be implemented.

, SP-SEC-Tax-2-3 - TSI-requirements are used to define a set of functions in order to achieve /increase IT-Security.

, SP-SEC-Tax-2-4 - Secure Component

An implementation, as part of an automation control system, either a host device, embedded device, network device or software application on a host device, which realizes subsystem functions, implements security capabilities and consisting of a physical encasing, computing capabilities and network communication, and interfacing to the Shared Cybersecurity Services.

Examples of CCS secure components are object controller, trackside cabinet, IXL rack, ATO-OB, OBU, ATO-TS, IXL/RBC combination, shared cybersecurity services, security proxy for legacy devices, …)

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

, SP-SEC-Tax-2-5 - Shared Cybersecurity Services (SCS)

A collection of standard security interfaces (SSIs) of central security functions accessible for all Secure Components in the automation solution. The realization of the Shared Cybersecurity Services (SCS) 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>.

, SP-SEC-Tax-2-6 - 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).

, SP-SEC-Tax-2-7 - 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.

, SP-SEC-Tax-2-8 - 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)

, SP-SEC-Tax-2-9 - 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.

, SP-SEC-Tax-2-10 - TLS endpoint

The TLS endpoint is a Secure Component using TLS-protected communication (client and server).

, SP-SEC-Tax-2-11 - OPC UA endpoint

The OPC UA endpoint is a Secure Component using OPC UA communication (client and server).

, SP-SEC-Tax-2-12 - HTTP endpoint

The HTTP endpoint is a Secure Component using HTTP communication (client and server).

, SP-SEC-Tax-2-13 - 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,...

, SP-SEC-Tax-2-14 - 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)

3 References

3.1.1 OPC UA Foundation

[OPC UA-10000-6]

OPC 10000-6: UA Part 6: Mappings

Hyperlinks	external reference - https://reference.opcfoundation.org/Core/Part6/v105/docs/

[OPC UA Profile SecurityPolicy [ECC-B] – ECC-nistP256]

Profile SecurityPolicy [ECC-B] – ECC-nistP256

Hyperlinks	external reference - http://opcfoundation.org/UA/SecurityPolicy#ECC_nistP256

[OPC UA Profile SecurityPolicy – ECC-brainpoolP256r1]

Profile SecurityPolicy – ECC-brainpoolP256r1

Hyperlinks	internal reference - http://opcfoundation.org/UA/SecurityPolicy#ECC_brainpoolP256r1

[OPC UA Profile SecurityPolicy [B] – Basic256Sha256]

SecurityPolicy [B] – Basic256Sha256

Hyperlinks	external reference - http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256

[OPC UA-10001-4 Amendment 4: ECC]

ECC for UACore 1.04

Hyperlinks	external reference - https://profiles.opcfoundation.org/document/122

3.1.2 IEC/ISO/CEN-CENELEC

[IEC 62443-2-1:2024]

Security program requirements for IACS asset owners

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/62883

[IEC 62443-2-4:2023]

Security program requirements for IACS service providers

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/67631

[IEC 62443-3-2:2020]

Security risk assessment for system design

Hyperlinks	internal reference - https://webstore.iec.ch/en/publication/30727

[IEC 62443-3-3:2013]

System security requirements and security levels

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/7033

[IEC 62443-4-1:2018]

Secure product development lifecycle requirements

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/33615

[IEC 62443-4-2:2019]

Technical security requirements for IACS components

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/34421

[CEN-CENELEC TS 50701:2023]

Railway applications - Cybersecurity

Hyperlinks	

[IEC PT 63452]

Railway applications - Cybersecurity - January 2025 draft

Hyperlinks	

[ISO/IEC 27001:2022]

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

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/79694

[ISO/IEC 27002:2022]

Information security, cybersecurity and privacy protection - Information security controls

Hyperlinks	external reference - https://webstore.iec.ch/en/publication/74287

3.1.3 IEEE

[IEEE 802.1X-2020]

IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control

Hyperlinks	external reference - https://standards.ieee.org/ieee/802.1X/7345/

[IEEE 802.1Q-2018]

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

Hyperlinks	internal reference - https://standards.ieee.org/ieee/802.1Q/6844/

3.1.4 IETF/RFC

[RFC 1952]

GZIP file format specification version 4.3

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc1952

[RFC 2865]

Remote Authentication Dial In User Service (RADIUS)

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc2865

[RFC 4086]

Randomness Requirements for Security

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc4086

[RFC 5280]

Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc5280

[RFC 5424]

The Syslog Protocol

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc5424

[RFC 5425]

Transport Layer Security (TLS) Transport Mapping for Syslog

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc5425

[RFC 5905]

Network Time Protocol Version 4: Protocol and Algorithms Specification

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc5905

[RFC 7636]

Proof Key for Code Exchange by OAuth Public Clients

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc7636

[RFC 7643]

System for Cross-domain Identity Management: Core Schema

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc7643

[RFC 7644]

System for Cross-domain Identity Management: Protocol

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc7644

[RFC 7858]

Specification for DNS over Transport Layer Security (TLS)

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc7858

[RFC 8176]

Authentication Method Reference Values

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc8176

[RFC 8446]

The Transport Layer Security (TLS) Protocol Version 1.3.

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc8446

[RFC 8915]

Network Time Security for the Network Time Protocol

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc8915

[RFC 9150]

TLS 1.3 Authentication and Integrity-Only Cipher Suites

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9150

[RFC 9190]

EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9190

[RFC 9364]

DNS Security Extensions (DNSSEC)

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9364

[RFC 9481]

Certificate Management Protocol (CMP) Algorithms

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9481

[RFC 9483]

Lightweight Certificate Management Protocol (CMP) Profile

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9483

[RFC 9662]

Updates to the Cipher Suites in Secure Syslog

Hyperlinks	external reference - https://datatracker.ietf.org/doc/html/rfc9662

[RFC automation-keyusages]

X.509 Certificate Extended Key Usage (EKU) for Automation

Note: this RFC is a draft, the actual RFC number will be added in a future version of this document

Hyperlinks	external reference - https://datatracker.ietf.org/doc/draft-ietf-lamps-automation-keyusages/

3.1.5 Legislation / Directives

[NIS2 Directive]

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

Hyperlinks	external reference - https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

[Cyber Resilience Act (CRA)]

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

Hyperlinks	external reference - https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[Cyber Security Act (CSA)]

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

Hyperlinks	external reference - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019R0881

[Radio Equipment Directive (RED)]

Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance

Hyperlinks	external reference - https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng

3.1.6 UNISIG Subsets

[UNISIG SUBSET-146 v4.00]

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

Hyperlinks	internal reference - https://www.era.europa.eu/system/files/2023-09/index010d_-_SUBSET-146_v400.pdf

[UNISIG SUBSET-147 v4.00]

CCS Consist network communication layer, V4.0

Hyperlinks	internal reference - https://www.era.europa.eu/system/files/2023-09/index090_-_SUBSET-147_v100.pdf

[UNISIG SUBSET-137 v4.00]

ETCS On-line Key Management, v4.0

Hyperlinks	internal reference - https://www.era.europa.eu/system/files/2023-09/index083_-_SUBSET-137_v400.pdf

3.1.7 ERTMS Users Group

[EUG Security Guideline]

The main objective of this document is the creation and presentation of Security Risk Assessment for System

Design process. This process is a harmonized and consolidated approach. This guideline was created in collaboration with EUG, RCA, EULYNX and OCORA.

Hyperlinks	external reference - https://ertms.be/wp-content/uploads/2023/11/EULYNX_EUG_RCA_OCORA_Security_Guideline_v2.03.pdf

[ERORAT Template]

EUG Risk Assessment Tool Excel based, aligned in EULYNX, EUG, RCA and OCORA.

Hyperlinks	external reference - https://ertms.be/wp-content/uploads/2023/07/ERORAT_Template_ZoneXX_v2.33_published.xlsx

[23E176: Procurement Guideline]

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

Hyperlinks	external reference - https://ertms.be/wp-content/uploads/2024/05/23E176-1A_Procurement_Guideline.pdf

[23E177: Security Logging Guideline]

The purpose of this document is to give guidance on architectural aspects of log data and SIEM infrastructures. Furthermore, corresponding processes are defined and explained.

Hyperlinks	external reference - https://ertms.be/wp-content/uploads/2024/11/23E177-2A-Security_Logging_SIEM_Guideline.pdf

[23E245: Security Penetration Testing]

The purpose of this document is to give guidance on penetration testing in the railway CCS domain (including EULYNX, ERTMS and the corresponding legacy systems).

Hyperlinks	external reference - https://ertms.be/wp-content/uploads/2024/10/23E245-1A_Security_Penetration_Testing.pdf

3.1.8 Other References

[EULYNX/EU-Rail BL4 R3]

Trackside asset specification

Hyperlinks	internal reference - https://rail-research.europa.eu/system_pillar/system-pillar-outputs/trackside-assets-specifications/

[OIDC 1.0]

OpenID Connect Core 1.0

Hyperlinks	external reference - https://openid.net/specs/openid-connect-core-1_0.html

[IANA SMI PKIX EKU]

SMI Security for PKIX Extended Key Purpose

Hyperlinks	external reference - https://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#smi-numbers-1.3.6.1.5.5.7.3

[IANA PENs]

Private Enterprise Numbers (PENs)

Hyperlinks	external reference - https://www.iana.org/assignments/enterprise-numbers/

[CLS:TS 50701:2023]

The CLC/TS 50701 standard contains several key aspects related to cyber security in railway applications

Hyperlinks	external reference - https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/

[MinElements_SBOM]

The Minimum Elements for an SBOM

Hyperlinks	internal reference - https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[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.

Hyperlinks	internal reference - https://www.cisecurity.org/cis-benchmarks

[I-STD-MAINTENANCE - SMI]

Description: Standard maintenance interface used for configuration distribution and activation. Offers cybersecurity and safety (according EN50129) mechanism for transferred data.

Transferred data:

- Orders and instructions regarding loading and activating new configurations
- Configurations that will be loaded on the target device
- Distribution feedback information

Hyperlinks	

3.1.9 System Pillar Cybersecurity Documents

[SP-SEC-CompSpec]

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

Hyperlinks	

[SP-SEC-CommSpec]

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

Hyperlinks	

[SP-SEC-ServSpec]

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

Hyperlinks	

[SP-SEC-PrgmReq]

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

Hyperlinks	

[SP-SEC-Tax]

Europe's Rail System Pillar Cybersecurity Domain - Taxonomy and References, v1.0

Hyperlinks	

[SP-SEC-DocTempl]

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

Hyperlinks	

[SP-SEC-ThreatCat]

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

Hyperlinks	

[SP-SEC-ThreatAna]

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

Hyperlinks	

[SP-SEC-RegCompl]

Europe's Rail SystemPillar Cybersecurity Domain - Regulatory Compliance Tracing, v1.0

Hyperlinks	

[SP-SEC-SuppEssFunc]

Europe's Rail SystemPillar Cybersecurity Domain - Support for essential functions, v1.0

Hyperlinks	

4 Document usage

, SP-SEC-Tax-4-1 - Item Type Definition

Item Type	Icon	Rationale
System Requirement		Used for mandatory requirements.
Text		Used for prose text, e.g. as an introduction or for additional information. The contents of these work items are **not requirements.**
Reference		Used for references to external documents. The contents of these work items are **not requirements.**
Definition		Used for term definitions. The contents of these work items are **not requirements.**