



EULYNX Initiative

EULYNX Security Concept

Document number: [Eu.Doc.15]

Version: 3.0 (0.A)

Contents

1	Introduction	1
1.1	Release information	1
1.2	Impressum	1
1.3	Purpose	2
1.4	Applicable standards and regulations	2
1.5	Applicable documents	2
1.6	Terms and abbreviations	3
1.7	Variability management	3
1.8	Definition of object types	3
2	Security for EULYNX	3
3	System under Consideration	3
4	Threat and Risk analysis	4
5	Security Architecture	4
5.1	Shared Cybersecurity Services (SCS)	4
5.2	Adaptions of SCS to EU-Rail Cybersecurity Specification	5
5.3	Securing Communication	6

ID	Type	Requirement
Eu.Sec.1	Head	1 Introduction
Eu.Sec.15	Head	1.1 Release information
Eu.Sec.5	Info	[Eu.Doc.15] EULYNX Security Concept CENELEC Phase: 2 Version: 3.0 (0.A) Approval date: 02.06.2025
Eu.Sec.6	Info	Version history
Eu.Sec.614	Info	version number: 2.0 (0.A) date: 17.05.2022 author: Robert Hughes, Ulrich Meier, Richard Poschinger, André Rumbold, Geir Rydland, Jaco Schoonen, Max Schubert, David Shipman review: CCB changes: editorial corrections and changes from CCB and UNIFE review
Eu.Sec.618	Info	version number: 2.1 (0.A) date: 28.06.2023 author: Ulrich Meier, Richard Poschinger, Nicolas Poyet, Max Schubert review: Security cluster + CCB changes: Full rework for Baseline 4 Release 2
Eu.Sec.653	Info	version number: 2.2 (0.A) date: 27.05.2025 author: Arwed Gölz, Richard Poschinger, Nicolas Poyet, André Rumbold, Max Schubert review: Security cluster changes: Full rework of Security Concept, adaption to align to EU-Rail Cybersecurity Specifications
Eu.Sec.668	Info	version number: 3.0 (0.A) date: 20.06.2025 author: Arwed Gölz, Richard Poschinger, Nicolas Poyet, André Rumbold, Max Schubert review: CCB changes: EUSEC-14
Eu.Sec.8	Head	1.2 Impressum
Eu.Sec.9	Info	Publisher: EULYNX Initiative A full list of the EULYNX Partners can be found on https://eulynx.eu/

ID	Type	Requirement
Eu.Sec.10	Info	Responsible for this document: EULYNX Project Management Office www.eulynx.eu
Eu.Sec.11	Info	Copyright EULYNX Partners All information included or disclosed in this document is licensed under the European Union Public Licence EUPL, Version 1.2 or later.
Eu.Sec.12	Head	1.3 Purpose
Eu.Sec.14	Info	This document provides the concept for security of the EULYNX System, with the application of EU-Rail Cybersecurity Specifications in EULYNX. This includes EULYNX security architecture, communication interfaces and systems themselves as well as required processes.
Eu.Sec.617	Info	The following security documents shall be used only as a complete set: <ul style="list-style-type: none"> • Eu.Doc.15 • EU-Rail Cybersecurity Specification V1.0 including <ul style="list-style-type: none"> • EU-Rail Secure Component Specification [SP-SEC-CompSpec] • EU-Rail Secure Communication Specification [SP-SEC-CommSpec] • EU-Rail Shared Cyber Security Services Specification [SP-SEC-ServSpec] • EU-Rail Secure Program Requirements [SP-SEC-PrgmReq] • The supporting documents of the EU-Rail Cybersecurity Specifications [SP-SEC-Support], including: <ul style="list-style-type: none"> • EU-Rail Initial Risk Assessment (EU-Rail identifier: SP-SEC-InitRiskAss) • EU-Rail Product Documentation Template (EU-Rail identifier: SP-SEC-PrdDocTmpl) • EU-Rail Regulatory Compliance (EU-Rail identifier: SP-SEC-RegCompl) • EU-Rail Support for Essential Functions (EU-Rail identifier: SP-SEC-SuppEssFunc) • EU-Rail System Description (EU-Rail identifier: SP-SEC-SysDesc) • EU-Rail Taxonomy and References (EU-Rail identifier: SP-SEC-Taxonomy-References) • EU-Rail Threat Catalogue (EU-Rail identifier: SP-SEC-ThreatCat)
Eu.Sec.16	Head	1.4 Applicable standards and regulations
Eu.Sec.211	Info	This document is using references as defined in the EU-Rail Security Taxonomy and References (part of [SP-SEC-Support]).
Eu.Sec.17	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].
Eu.Sec.18	Head	1.5 Applicable documents
Eu.Sec.19	Info	The current versions of EULYNX documents used as input or related to this document are listed in the EULYNX Documentation Plan [Eu.Doc.11]. The relationships between the documents are displayed in the Appendix A1 Documentation plan and structure [Eu.Doc.11_A1].
Eu.Sec.667	Info	Further explanations and recommendations on EULYNX Security will be provided in the EULYNX Security Guideline [Eu.Doc.125].

ID	Type	Requirement
Eu.Sec.654	Info	<p>Further guidance on security is published by the Rail Security Expert Group (RSEG) on the website of the ERTMS Users Group (https://ertms.be).</p> <p>The RSEG consists of security experts of the following groups:</p> <ul style="list-style-type: none"> • EULYNX Security Cluster – Part of the EULYNX Initiative • ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
Eu.Sec.20	Head	1.6 Terms and abbreviations
Eu.Sec.21	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9] and EU-Rail Security Taxonomy and References (part of [SP-SEC-Support]).
Eu.Sec.22	Head	1.7 Variability management
Eu.Sec.23	Info	This document is valid for the complete EULYNX System. Variability management is not used in this document.
Eu.Sec.24	Head	1.8 Definition of object types
Eu.Sec.25	Info	The following definition for object types is applied in this document:
Eu.Sec.26	Info	<ul style="list-style-type: none"> • "Req" - This denotes a mandatory requirement.
Eu.Sec.27	Info	<ul style="list-style-type: none"> • "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.
Eu.Sec.28	Info	<ul style="list-style-type: none"> • "Head" - This denotes chapter headings.
Eu.Sec.3	Head	2 Security for EULYNX
Eu.Sec.220	Info	The Security Concept addresses technical and processual aspects. It follows the EULYNX project definition and respects the interface specifications.
Eu.Sec.222	Info	The architecture of EULYNX and the according interfaces can be found in the EULYNX System Definition - Appendix A1 [Eu.Doc.7_A1].
Eu.Sec.317	Head	3 System under Consideration
Eu.Sec.318	Info	The EULYNX architecture, shown in the EULYNX System Definition - Appendix A1 [Eu.Doc.7_A1] is the system under consideration. Additional components of surrounding systems/components are taken into the definition as they are vital for the implementation. The system under consideration (SuC) is the basis for defining zones and conduits.

ID	Type	Requirement
Eu.Sec.352	Head	4 Threat and Risk analysis
Eu.Sec.285	Info	To analyse the risks in the EULYNX architecture and define mitigating measures, the ERORAT Guideline of EUG, RCA, OCORA and EULYNX is used (available on the EUG website, http://ertms.be). The method defined in the guideline is based on IEC 62443 and the associated extension regarding railway-specific aspects in the standard TS 50701. This is done in Phase 3 (risk assessment) of the CENELEC process. The risk assessment results were input to the EU-Rail Cybersecurity Specification (as listed in the Introduction Chapter). EU-Rail decided on using the same risk assessment method. The risk assessment is to be updated regularly according to current status of threats and vulnerabilities as a life-cycle-management task as a joined effort of the EULYNX Security Cluster and the EU-Rail SP Security Group.
Eu.Sec.286	Info	The process defined in the ERORAT Guideline is started by defining the systems under consideration. Thus, the scope of the assessment is determined. Based on this the zones and conduits can be defined, giving a structured overview over the scope.
Eu.Sec.355	Head	5 Security Architecture
Eu.Sec.357	Info	The EULYNX System architecture [Eu.Doc.7_A1] is applied regarding security according to the following definitions: <ul style="list-style-type: none"> • All EULYNX subsystems are Secure Components according to the definition of [SP-SEC-CompSpec] • The Subsystem - Security Services Platform (SSP) is equivalent to the Shared Cybersecurity Services (SCS) according to the definition of [SP-SEC-ServSpec] • Connected non-EULYNX systems can either be implemented as Secure Components (recommended) or as (insecure) Legacy Components connected via a Security Proxy implemented as a Secure Component as shown in the System Description of [SP-SEC-Support]
Eu.Sec.365	Head	5.1 Shared Cybersecurity Services (SCS)
Eu.Sec.369	Info	Requirements for the Shared Cybersecurity Services (SCS) and the Standard Security Interfaces (SSI) are specified in [SP-SEC-ServSpec].
Eu.Sec.370	Info	The security services are available via SSI to every EULYNX subsystem. Furthermore, security services are available to those adjacent systems that communicate with EULYNX subsystems via SCI.
Eu.Sec.371	Info	The following applicability of SSI service functions for EULYNX subsystems is defined:
Eu.Sec.656	Info	Required services: <ul style="list-style-type: none"> • STS: Secure Time Synchronisation • PKI: Public Key Infrastructure • IAM: Identity and Access Management • NAC: Network Access Control • LOG: Security Logging • MNT: Security Maintenance

ID	Type	Requirement
Eu.Sec.657	Info	Partially required services: <ul style="list-style-type: none"> • BKP: Backup and Restore <ul style="list-style-type: none"> • not required by EfeS and EIL • required by MDM • required by SCS (as defined [SP-SEC-ServSpec]) • UAS: User Authentication Service <ul style="list-style-type: none"> • not required by EfeS • required if direct human user access is provided in other subsystems or adjacent systems
Eu.Sec.658	Info	Not required services: <ul style="list-style-type: none"> • DNS: Domain Name System
Eu.Sec.659	Head	5.2 Adaptions of SCS to EU-Rail Cybersecurity Specification
Eu.Sec.660	Info	Changes for each SSI service function between the previous EULYNX BL4R3 and the current EULYNX BL4R4 (including the EU-Rail Cybersecurity Specification v1.0) are displayed below:

ID	Type	Requirement
Eu.Sec.661	Info	<ul style="list-style-type: none"> • STS: Secure Time Synchronisation <ul style="list-style-type: none"> • Change from NTP to NTS • No conflict, as NTS is backwards compatible to NTP • PKI: Public Key Infrastructure <ul style="list-style-type: none"> • EST and OCSP removed • CMP and CRL remain • CMP applied with LCMP profile, no conflict • Certificate Profiles defined, migration possible with same PKI structure • IAM: Identity and Access Management <ul style="list-style-type: none"> • Newly standardised interface • Authentication via certificates for OPC UA remains • Authorisation is performed using IAM • NAC: Network Access Control <ul style="list-style-type: none"> • No change • LOG: Security Logging <ul style="list-style-type: none"> • No change on interface level • Log message definition was changed, migration only affects SIEM • MNT: Security Maintenance <ul style="list-style-type: none"> • Newly standardised interface • BKP: Backup and Restore <ul style="list-style-type: none"> • Newly standardised interface • Affects only a limited number of centralised services, no impact on e.g. EfeS • UAS: User Authentication Service <ul style="list-style-type: none"> • Newly standardised interface • DNS: Domain Name System <ul style="list-style-type: none"> • Not used in EULYNX
Eu.Sec.437	Head	5.3 Securing Communication
Eu.Sec.662	Info	All interfaces specified in EULYNX are protected using the requirements of [SP-SEC-CommSpec].
Eu.Sec.663	Info	For SCI the [SP-SEC-CommSpec] provides the option to use encrypting ciphers and integrity-only ciphers.
Eu.Sec.664	Info	The IM has to decide if the usage of integrity-only ciphers is allowed.
Eu.Sec.665	Info	Integrity-only ciphers leave more implementation options for Intrusion Detection and Juridical Recording (e.g. integration of these functionalities in Subsystem - Communication System).
Eu.Sec.666	Info	On the other hand, the usage of integrity-only ciphers facilitates the reconnaissance phase for adversaries.