



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	1
1.4	Applicable standards and regulations	2
1.5	Applicable documents	3
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	V 3.0 (0.A) > V 2.1 (0.A)
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	Object Text: [Eu.Doc.15] EULYNX Security Concept CENELEC Phase: 2 Version: 2 3. 1 0 (0.A) Approval date: 15 02.06. 2023 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	object created after baseline 2.1 (0.A)
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	object created after baseline 2.1 (0.A)
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/	Object Text: Publisher: EULYNX Initiative A full list of the EULYNX Partners can be found on www. https://eulynx.eu/index.php/members
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	

ID	Type	Requirement	V 3.0 (0.A) > V 2.1 (0.A)
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.	Object Text: The purpose of this This document is to define provides the security requirements on concept-level for the security whole of the EULYNX architecture System, including communication interfaces and with system the components application themselves of as EU-Rail well Cybersecurity as Specifications required in processes EULYNX. This includes the whole EULYNX security life architecture, cycle communication from interfaces system and definition systems up themselves to as decommissioning well of as the required system 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-PrdDocTpl) • 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) 	Object Text: The following statements should be considered before applying the specification: • The security documents of the following enumeration shall be referred and used only as a complete set: — • Eu.Doc.15 — • EU-Rail Eu.Doc.114 — Cybersecurity eSpecification Eu.DocV1.1150 including • Eu.Doc.116 EU-Rail Secure Component Specification [SP-SEC-CompSpec] — • Eu.Doc.117 • EU-Rail Secure Communication Specification [SP-SEC-CommSpec] — • Eu.Doc.121 • Development EU-Rail of Shared the Cyber specification Security is Services based Specification on [SP-SEC-ServSpec] _ IEC 62443 process, • together EU-Rail with Secure TS Program 50701 Requirements railway [SP-SEC-PrgmReq] _ specification application suggestions: • If The the supporting infrastructure documents manager of (IM) the applies EU-Rail the Cybersecurity Security Specifications Specification [SP-SEC-Support], the including: IM must be aware • that EU-Rail successful Initial implementation Risk requires Assessment a (EU-Rail detailed identifier: analysis SP-SEC-InitRiskAss) and adoption of, at least, the IM's • rollout EU-Rail and Product maintenance Documentation procedures: • Template The (EU-Rail specifications identifier: contains SP-SEC-PrdDocTpl) options that need to be decided carefully • by EU-Rail the Regulatory IM Compliance due (EU-Rail to identifier: impact SP-SEC-RegCompl) to feasibility in migration, business activity, process • adoption EU-Rail Support for operation Essential Functions (rollout, EU-Rail maintenance,...), identifier: tender SP-SEC-SuppEssFunc) process, possible suppliers, and costs (CAPEX, OPEX): • The EU-Rail current System specification Description does (EU-Rail not identifier: contain SP-SEC-SysDesc) testing requirements for the suppliers. So, the • test EU-Rail type Taxonomy (testing, and audit, References analysis, (EU-Rail demonstration identifier: SP-SEC-Taxonomy-References) and its acceptance criteria should be defined • before EU-Rail using Threat the Catalogue documents (EU-Rail in identifier: tender SP-SEC-ThreatCat) process:
Eu.Sec.16	Head	1.4 Applicable standards and regulations	

ID	Type	Requirement	V 3.0 (0.A) > V 2.1 (0.A)
Eu.Sec.211	Info	This document is using references as defined in the EU-Rail Security Taxonomy and References (part of [SP-SEC-Support]).	Object Text: This document refers to the most specific standards, written for railways. Other standards are only referenced, is if using there references areas gaps defined in the definition of the railway specific standards. This ensures, that only the difference between the most specific standard and the final EU-Rail security Security architecture Taxonomy and requirements specification needs to be described References in (part this of document [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].	object created after baseline 2.1 (0.A)
Eu.Sec.654	Info	Further guidance on security is published by the Rail Security Expert Group (RSEG) on the website of the ERTMS Users Group (https://ertms.be). The RSEG consists of security experts of the following groups: <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	object created after baseline 2.1 (0.A)
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]).	Object Text: 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	• "Req" - This denotes a mandatory requirement.	
Eu.Sec.27	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.	
Eu.Sec.28	Info	• "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.	Object Text: The Security Concept addresses technical and processual aspects. The concept 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.	Object Text: The EULYNX architecture, shown in the EULYNX System Definition - Appendix A1 [Eu.Doc.7_A1] is the system under consideration. Additional

ID	Type	Requirement	V 3.0 (0.A) > V 2.1 (0.A)
			<p>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. The goal is to group systems or components into zones and conduits that have the same requirements from the security point of view, due to similar threats and possible impacts. If two components or sub-systems have same requirements but are connected via an untrusted network connection or a connection that does not have the same requirements, they must be split into two different zones, connected through a conduit. Thus, zones over one system with different locations, are not possible.</p> <p>Note: Security zones are not automatically networks.</p>
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.	<p>Object Text: To analyse the risks in the EULYNX architecture and define mitigating measures, the SecurityERORAT 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. <u>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.</u> The risk assessment is to be updated regularly according to current status of threats and vulnerabilities as a life-cycle-management task <u>as a joined effort of the EULYNX Security Cluster and the EU-Rail SP Security Group.</u></p>
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.	<p>Object Text: The process defined in the guidelineERORAT 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.</p>
Eu.Sec.355	Head	5 Security Architecture	
Eu.Sec.357	Info	<p>The EULYNX System architecture [Eu.Doc.7_A1] is applied regarding security according to the following definitions:</p> <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] 	<p>Object Text: The technicalEULYNX System architecture for[Eu.Doc.7_A1] is applied regarding security according to the following definitions:</p> <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 basedequivalent onto the architectureShared forCybersecurity Services (SCS) according to the definition of [SP-SEC-ServSpec] • Connected non-EULYNX; referencedsystems 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 Chapterthe 2.System Description of [SP-SEC-Support]
Eu.Sec.365	Head	5.1 Shared Cybersecurity Services (SCS)	<p>Object Heading: SSIShared StandardCybersecurity SecurityServices Interfaces(SCS)</p>
Eu.Sec.369	Info	Requirements for the Shared Cybersecurity Services (SCS) and the Standard Security Interfaces (SSI) are specified in [SP-SEC-ServSpec].	<p>Object Text: Security requirementsRequirements for allthe subservicesShared ofCybersecurity Services (SCS) and the Standard Security InterfaceInterfaces (SSI) are givenspecified in the EULYNX Security-Parameter Specification [Eu.Doc.115SP-SEC-ServSpec].</p>

ID	Type	Requirement	V 3.0 (0.A) > V 2.1 (0.A)
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.	Object Text: The security services are available for <u>via SSI to</u> every EULYNX device <u>subsystem</u> . 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:	Object Text: The security <u>following services</u> applicability are <u>of briefly</u> SSI described <u>service in</u> functions the <u>for following</u> EULYNX sections <u>subsystems</u> 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 	object created after baseline 2.1 (0.A)
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 	object created after baseline 2.1 (0.A)
Eu.Sec.658	Info	Not required services: <ul style="list-style-type: none"> • DNS: Domain Name System 	object created after baseline 2.1 (0.A)
Eu.Sec.659	Head	5.2 Adaptions of SCS to EU-Rail Cybersecurity Specification	object created after baseline 2.1 (0.A)
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:	object created after baseline 2.1 (0.A)

ID	Type	Requirement	V 3.0 (0.A) > V 2.1 (0.A)
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	object created after baseline 2.1 (0.A)
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].	object created after baseline 2.1 (0.A)
Eu.Sec.663	Info	For SCI the [SP-SEC-CommSpec] provides the option to use encrypting ciphers and integrity-only ciphers.	object created after baseline 2.1 (0.A)
Eu.Sec.664	Info	The IM has to decide if the usage of integrity-only ciphers is allowed.	object created after baseline 2.1 (0.A)
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).	object created after baseline 2.1 (0.A)
Eu.Sec.666	Info	On the other hand, the usage of integrity-only ciphers facilitates the reconnaissance phase for adversaries.	object created after baseline 2.1 (0.A)