



EULYNX Initiative

EULYNX Security Concept

Document number: [Eu.Doc.15]
Version: 2.1 (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	2
1.6	Terms and abbreviations	3
1.7	Variability management	3
1.8	Definition of object types	3
2	Security for EULYNX	3
2.1	Legal requirements from NIS directive	3
2.2	Security Strategy for Railway Operation	3
2.2.1	Mitigation strategies	3
2.2.2	Security and safety considerations for Railway Operations	3
2.2.2.1	Areas of conflict	3
2.2.2.2	Resolution of conflicts	5
2.3	Threat definition	5
2.4	Security principles	5
2.4.1	Secure by design	5
2.4.2	Defence in depth	6
2.4.3	Secure by Default	6
2.4.4	Simplicity over Complexity	6
2.4.5	Assume Failure & Compromise	7
2.4.6	Fail Safe and Secure	7
2.4.7	Zero Trust	7
2.4.8	Least Privilege	7
2.4.9	Usability & Manageability	8
2.4.10	Design for Automation	8
2.4.11	Open Design	8
2.5	Process definition	8
2.6	Constraints in Standards for Safety and Security	9
2.7	Assumption on available or to be established security services	9
2.7.1	Security Operations Centre (SOC)	9
2.7.2	Security Incident and Event Management (SIEM)	10
2.7.3	Security Incident Centre (SIC)	10
2.7.4	Cyber security incident response team (CSIRT)	10
2.7.5	Information Sharing and Analysis Centre (ISAC)	10

2.8	Conformity to standard IEC 62443	10
2.9	Information Security Management System	10
3	Analyses	10
3.1	Assumptions / General requirements	10
3.2	System under Consideration	11
3.2.1	Electronic Interlocking (EIL)	12
3.2.2	EULYNX field element Subsystems (EfeS)	12
3.2.3	Maintenance and Data Management (MDM)	13
3.2.4	Trackside Assets (TA)	13
3.2.5	Traffic Control System (TCS)	13
3.2.6	ILS-Adapter	13
3.2.7	Maintenance User Interface (MaintUI)	13
3.2.8	Operational User Interface (OpUI)	13
3.2.9	ETCS Radio Block Centre (RBC)	13
3.2.10	Adjacent (legacy) EIL	13
3.2.11	Subsystem Communication System (SCS)	14
3.3	Threat and Risk analysis	14
4	Security Architecture	14
4.1	Technical architecture and interfaces	14
4.1.1	SSI Standard Security Interfaces	15
4.1.2	Security Services Platform (SSP)	15
4.1.2.1	Security Incident Detection	15
4.1.2.1.1	Security Logging Service	15
4.1.2.1.2	SIEM	15
4.1.2.2	Backup	15
4.1.2.3	Identity and Access Management (IAM)	15
4.1.2.4	Public Key Infrastructure (PKI)	15
4.1.3	Shared Supportive Services	16
4.1.3.1	Asset Inventory	16
4.1.3.2	Software and Configuration Repository	16
4.1.3.3	Diagnostics collector	17
4.1.4	Zone Model	17
4.1.5	Securing Communication	17
4.1.5.1	Requirements for safety related communication	17
4.1.5.2	Protection solutions / concepts (Variant A, B, C)	18
4.1.5.2.1	Basic concept of Variant A, B, C	18
4.1.5.2.2	Variant A "Crypto Box"	20
4.1.5.2.3	Variant B and C common requirements	21
4.1.5.2.4	Variant B specific requirement: "TLS with dedicated hardware board"	21
4.1.5.2.5	Variant C specific requirement: "TLS with software separation"	22
4.1.5.2.6	Physical protection for Variants A, B, and C	23

4.1.5.2.6.1	Physical protection for Variant A	23
4.1.5.2.6.2	Physical protection for Variant B	23
4.1.5.2.6.3	Physical protection for Variant C	24
4.1.5.2.6.4	Physical defence in depth	24
4.1.5.2.7	Connection Manager	25
4.1.5.2.8	Reference points	25
4.1.5.3	Communication models and migration	25
4.1.5.4	Security for PDI layer	27
4.1.5.4.1	Variant A:	27
4.1.5.4.2	Variant B and C:	28
4.2	Process architecture	28

ID	Type	Requirement	Valid for
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: 2.1 (0.A) Approval date: 15.06.2023	--
Eu.Sec.6	Info	Version history	--
Eu.Sec.205	Info	version number: 1.0 (0.A) date: 23.06.2020 author: Max Schubert, Nico Huurman review: CCB changes: EUSEC-1, EUSEC-2, EUSEC-3	--
Eu.Sec.209	Info	version number: 1.1 (0.A) date: 22.12.2021 author: Robert Hughes, Ulrich Meier, Richard Poschinger, André Rumbold, Geir Rydland, Jaco Schoonen, Max Schubert, David Shipman review: security cluster changes: Full rework for Baseline 4	--
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.8	Head	1.2 Impressum	
Eu.Sec.9	Info	Publisher: EULYNX Initiative A full list of the EULYNX Partners can be found on www.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	
Eu.Sec.14	Info	The purpose of this document is to define the security requirements on concept level for the whole EULYNX architecture, including communication interfaces and system components themselves as well as required processes. This includes the whole security life cycle from system definition up to decommissioning of the system.	--
Eu.Sec.210	Info	The technical requirements for security are specified in the EULYNX Security specification [Eu.Doc.114]	--
Eu.Sec.13	Info	Inputs for the document are the systems operational environment, applicable security standards as well as purpose and scope of the system.	--
Eu.Sec.30	Info	Having a security concept at EULYNX level will facilitate alignment with other infrastructure managers and European bodies, because the same language and terminology is used.	--

ID	Type	Requirement	Valid for
Eu.Sec.612	Info	This document is intended for the following users: <ul style="list-style-type: none"> • safety authorities • infrastructure managers • safety assessors • signalling system suppliers • validators • security assessors 	--
Eu.Sec.613	Info	The applicability of each requirement either exclusively for the infrastructure manager or for all relevant parties is indicated by the column "Valid for". Note: 'All parties' may include suppliers of signalling system components and suppliers of other components dedicated to IT security.	--
Eu.Sec.617	Info	The following statements should be considered before applying the specification: <ul style="list-style-type: none"> • The security documents of the following enumeration shall be referred and used only as a complete set. <ul style="list-style-type: none"> o Eu.Doc.15 o Eu.Doc.114 o Eu.Doc.115 o Eu.Doc.116 o Eu.Doc.117 o Eu.Doc.121 • Development of the specification is based on IEC 62443 process, together with TS 50701 railway specification application suggestions. • If the infrastructure manager (IM) applies the Security Specification, the IM must be aware that successful implementation requires a detailed analysis and adoption of, at least, the IM's rollout and maintenance procedures. • The specifications contains options that need to be decided carefully by the IM due to impact to feasibility in migration, business activity, process adoption for operation (rollout, maintenance,...), tender process, possible suppliers, and costs (CAPEX, OPEX). • The current specification does not contain testing requirements for the suppliers. So, the test type (testing, audit, analysis, demonstration) and its acceptance criteria should be defined before using the documents in tender process. 	--
Eu.Sec.16	Head	1.4 Applicable standards and regulations	
Eu.Sec.211	Info	This document refers to the most specific standards, written for railways. Other standards are only referenced, if there are gaps in the definition of the railway specific standards. This ensures, that only the difference between the most specific standard and the final security architecture and requirements specification needs to be described in this document.	--
Eu.Sec.212	Info	Standards referred by these railway standards are not referred.	--
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.215	Info	This document is written based on the following standards: <ol style="list-style-type: none"> 1) TS 50701 [EU.Ref.191] 2) IEC 62443 [EU.Ref.35] <ul style="list-style-type: none"> IEC 62443-2-1 IEC 62443-2-4 IEC 62443-3-2 IEC 62443-3-3 IEC 62443-4-1 IEC 62443-4-2 3) EN 50159 [EU.Ref.52] 4) EN 50126 [EU.Ref.49] 5) EN 50128 [EU.Ref.50] 6) EN 50129 [EU.Ref.51] 7) ISO 27001 [EU.Ref.189] <p>If requirements in these standards conflict, the lower number overrules the higher number. This does not result in an obligation for the IM to implement standards mentioned above.</p>	--
Eu.Sec.216	Info	If one of the referenced standards shall be applied in addition to requirements in this document, it is stated explicitly.	--
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].	--

ID	Type	Requirement	Valid for
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].	--
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. The concept 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.59	Head	2.1 Legal requirements from NIS directive	
Eu.Sec.60	Info	Since the NIS Directives are in force for countries of the European Union, they have an impact on the Critical Infrastructures of these countries as they pose several requirements on these.	--
Eu.Sec.61	Info	As an operator of essential services (if classified as such) the railway operator shall:	--
Eu.Sec.62	Info	<ul style="list-style-type: none">Prevent risks by taking technical and organisational measures according to a certain defined level of security proportionate to the risk.	--
Eu.Sec.64	Info	<ul style="list-style-type: none">Handle incidents, which means that he prevents and minimises the impact of incidents on the IT systems used.	--
Eu.Sec.65	Info	<ul style="list-style-type: none">Reports notifiable incidents according to the number of affected users, duration of the incident and the geographic spread.	--
Eu.Sec.33	Head	2.2 Security Strategy for Railway Operation	
Eu.Sec.223	Info	This chapter defines the general strategies for mitigation of risks and specification of measures.	--
Eu.Sec.224	Head	2.2.1 Mitigation strategies	
Eu.Sec.225	Info	Ranking for the mitigation of risks is defined (based on losses): 1. Priority: Eliminate hazard or threat. 2. Priority: Be resilient against the risk using e.g. adequate processes and architecture. 3. Priority: Define mitigating actions 4. Priority: Accept risk and integrate the risk in overall risk management (or Safety Management System). 5. Priority: Transfer to assurance	--
Eu.Sec.226	Head	2.2.2 Security and safety considerations for Railway Operations	
Eu.Sec.227	Info	The EULYNX security documents are based on following assumptions on areas of conflict in safety and security which result in the overall concept as “resolution of conflicts”.	--
Eu.Sec.228	Head	2.2.2.1 Areas of conflict	
Eu.Sec.229	Info	Areas of conflict	--

ID	Type	Requirement			Valid for
			Safety	Security	
		Trust vs. Zero trust	Unconditional trust within the whole system The system was designed and tested/certified by a competent body. All aspects considered correctly. If the operator follows the requirements (technical, processual, controls), nothing bad can happen. Everyone is acting as requested!	Miss-trust / Zero trust No trust until a defined level of trust is established. There are people intentionally not following the requirements (e.g. to ease their work or to attack)	
		Fail Safe & Secure	The system never should harm itself or the environment. In case of doubt or failure it enters automatically into a “safe state”. Based on Safety Integrity Levels based on standard’s definition.	If a security control fails, it should maintain a state of deny access. Design security mechanisms so that a failure will follow the same execution path as disallowing the operation. Prevent unauthorized access in case of errors, failures, exceptions, system degradation, or compromise. Primary goal is ensuring system’s integrity.	
		Monitoring & Logging	Detecting errors/failures is time critical as safety might be affected. There are only technical failures and considered wrongdoings. All safety-relevant failures are detected, a timely reaction is performed, or initiated, by the system itself or by the superior system.	Systems are monitored to detect failures with respect to operational levels/availability. Failures/errors might indicate an attack or wrongdoing; however, a detection of an attack/wrongdoing might not be possible.	
		Defense in Depth	There are no attackers. The whole system is located in a controlled environment. Intentional wrongdoings are excluded.	There are attackers, from outside and inside. Every (sub-) system must establish the security controls on several layers to protect against outside and inside attacks.	
Eu.Sec.615	Info	Areas of conflict			--

ID	Type	Requirement			Valid for
			Safety	Security	
		Simplicity over Complexity	Safety relevant systems are designed only for that very task, only contain the minimum required to implement the defined safety functionality.	Security systems must be tailored to the task as these systems/libraries include many options. The systems are highly complex and as a result faulty. The tailoring is done usually during system integration and not during the design phase. This tailoring changes over time due to changing threat landscape.	
		Assume failure and compromise	Failure states are detected in a timely manner. Compromising a system is impossible due to requirements and controls.	It is very likely that an attack is not detected in a timely manner. Compromising a system is possible all the time. Both could potentially be detected years later.	
		Open Design	Highly integrated, proprietary/closed designed systems. 100% control of the system and its design reduces the risk in the approval process. The supplier guaranties the safety functionality and spare parts for decades.	Open standards and designs are preferred. Close or proprietary protocols and interfaces are per se considered insecure, as no independent testing can take place.	
		Maintainability / Availability / Updates	There is no need for updates as long as everything was considered correctly, and the test procedures were not faulty. The system is operated in a deterministic environment, hence there are no unconsidered coincidences. Every change requires a new certification/homologation.	As security erodes over time, updates are required. Newly detected security vulnerabilities must be mitigated. Both leads to updating system and protective concepts. This is the only way to ensure system/information integrity.	
Eu.Sec.230	Info	Implementing the "fail secure" or "fail safe" principle affects availability negatively. For a safety system, system integrity is key and is the basis for all assessments and certifications. A "fail open" action can therefore never be accepted for safety or safety-related systems or functionality. Depending on architecture and technical implementation, following the "fail open" principle is only acceptable, if system integrity for safety is not affected and ensured by design of the system.			--
Eu.Sec.231	Head	2.2.2.2 Resolution of conflicts			
Eu.Sec.232	Info	As the areas of conflict cannot be eliminated in general, the analysis of all RAMSS (Reliability, Availability, Maintainability, Safety and Security) aspects must be done together. The method of "separation of concerns" can be followed if interactions/conflicts are identified and solved. Defining them as out-of-scope is not an option.			--
Eu.Sec.233	Info	Security must start with the information used end-to-end, e.g., this is the top-level control loop if a System-Theoretic Process Analysis (STPA) method is applied and following the information flow defined by the processes. These processes involve business delivery processes and operational technology control loops.			--
Eu.Sec.234	Info	As security affects safety and RAM aspects, a security protection profile must include all RAMS aspects, hence there is only one protection profile.			--
Eu.Sec.40	Head	2.3 Threat definition			
Eu.Sec.41	Info	In the EULYNX assurance approach, the term "threat" is used to denote a threat to the assurability of the EULYNX solution. This is not to be confused with the use of "threat" in the security domain. Therefore, in this document we refer to both Assurance Threats and Security Threats. If not otherwise stated, the term "threat" in this document refers to a Security Threat.			--
Eu.Sec.43	Head	2.4 Security principles			
Eu.Sec.235	Info	The security principles followed in the concept and related specification documents are listed in the following sections.			--
Eu.Sec.236	Head	2.4.1 Secure by design			

ID	Type	Requirement	Valid for
Eu.Sec.237	Info	Make security part of requirements, and not an afterthought	--
Eu.Sec.238	Info	Rationale Protect a business application or information system against attacks by considering security requirements as part of its overall requirements. <ul style="list-style-type: none"> • Experience has shown it is both costly and difficult to implement security measures after a system has been developed. • Avoid unnecessary development efforts by considering security requirements early on. • As security interferes with safety (e.g. timings, fail behaviour) they must be a holistic approach. 	--
Eu.Sec.239	Info	Implications <ul style="list-style-type: none"> • Understand the resulting security requirements in the engineering, design, implementation, and disposal of the system. • Security should treat the root cause of a problem, not its symptom. 	--
Eu.Sec.240	Head	2.4.2 Defence in depth	
Eu.Sec.241	Info	Avoid reliance on a single type of security control	--
Eu.Sec.242	Info	Rationale Implementing security on multiple layers is better than relying on a single defence layer. If one security control fails or is bypassed, an additional layer can help preventing the attack. <ul style="list-style-type: none"> • Identify and secure the weakest links first. • Use multiple security layers to increase effort for an attacker to compromise a system or application. 	--
Eu.Sec.243	Info	Implications <ul style="list-style-type: none"> • Create a security architecture that documents the different layers of protection. • Balance defence in depth against simplicity and business needs. • Each deeper security layer should not trust the previous layers. • Compartmentalize the system by defining security boundaries for information flows. • Prepare for the worst possible compromise scenario. 	--
Eu.Sec.244	Head	2.4.3 Secure by Default	
Eu.Sec.245	Info	Set secure default options to limit inherent security vulnerabilities	--
Eu.Sec.246	Info	Rationale System or application configurations should favour security over not being secure. The default setting for a security control should be to deny access to a resource and require a configuration to specifically grant access. When the system goes into an error or exception state, these states must favour security over not being secure.	--
Eu.Sec.247	Info	Implications <ul style="list-style-type: none"> • Security should not require extensive configuration to work and should just work reliably where implemented. • Establish secure defaults when system starts or goes in error or exception states. • Provide least privilege or make only necessary services and features available. • Use integrity protection and encryption by default for both data at rest and in transit. Omit encryption only if confidentiality protection is not required. 	--
Eu.Sec.248	Head	2.4.4 Simplicity over Complexity	
Eu.Sec.249	Info	Complexity is the worst enemy of security	--
Eu.Sec.250	Info	Rationale Complexity in systems leads to increased human confusion, errors, vulnerabilities, automation failures, and difficulty of recovering from an issue. Favour simple and consistent architectures, designs, and implementations. Avoid unnecessary complexity. The more complex the system, the more likely it may possess exploitable flaws	--
Eu.Sec.251	Info	Implications <ul style="list-style-type: none"> • Simplicity should be a key objective in design of systems and security. • DRY - do not repeat yourself. • Reduce the variety and types of hardware and software types and versions. • Designing systems that use the least hardware and software resources possible. • Favour convention over configuration. • Do not implement unnecessary security mechanisms. • Complexity makes vulnerabilities harder for developers and testers to uncover. Each feature, function, and interaction are a potential threat vector. • Complexity makes vulnerabilities harder to fix once we find them. 	--

ID	Type	Requirement	Valid for
Eu.Sec.252	Info	Notes <ul style="list-style-type: none">Do not oversimplify.Balance reduced complexity against diversity required to achieve resiliency and reduced single-point-of-failures.	--
Eu.Sec.253	Head	2.4.5 Assume Failure & Compromise	
Eu.Sec.254	Info	Complex distributed systems lead to unpredictability and cascading failures	--
Eu.Sec.255	Info	Rationale We build and operate highly coupled and interactively complex systems. Even when all the individual components of complex system are functioning properly, the interactions between those components can cause unpredictable outcomes and vulnerabilities. Rare or surprising combinations of events, vulnerabilities, and creative user interactions make such systems difficult to predict. Prediction, complete testing, and modelling of all states is not possible in such systems, we therefore must assume and account for failures and compromise.	--
Eu.Sec.256	Info	Implications <ul style="list-style-type: none">Our systems are too complex to anticipate all potential interactions or vulnerabilities.Assume that critical parts of the infrastructure can be compromised during the life-cycle of the components and systems .Embrace principles of resilient engineering and testing - facilitate real and repeated tests to uncover systemic weaknesses.Design system for automated testability.Establish continued and comprehensive monitoring of vital parameters to determine system health and security.Security shall actively managed over the IACS and product life-cycle.	--
Eu.Sec.257	Head	2.4.6 Fail Safe and Secure	
Eu.Sec.258	Info	Failures should lead to a safe and secure state. Risk does not hurt - the impact does	--
Eu.Sec.259	Info	Rationale If a security control fails, it should maintain a state of deny access. Design security mechanisms so that a failure will follow the same execution path as disallowing the operation. Prevent unauthorized access in case of errors, failures, exceptions, system degradation, or compromise.	--
Eu.Sec.260	Info	Implications <ul style="list-style-type: none">Design to minimize the impact of component or control failures or compromise.Confidentiality and integrity assurance top availability assurance.Security methods like isAuthorized(), isAuthenticated(), and validate() should all return false if there is an exception during processing.Assume system failure & compromise in design decisions.	--
Eu.Sec.261	Info	Examples <ul style="list-style-type: none">Dead man’s switch is automatically operated if the human operator becomes incapacitated.Traffic light controllers use a Conflict Monitor Unit to detect faults or conflicting signals and switch an intersection to an all flashing error signal, rather than displaying potentially dangerous conflicting signals.	--
Eu.Sec.262	Head	2.4.7 Zero Trust	
Eu.Sec.263	Info	Assume everything to be insecure until a level of trust is established	--
Eu.Sec.264	Info	Rationale The historic concept of trust that is based on a perimeter separating the inside from the outside does no longer hold in today’s rapidly changing environment. Assuming no trust is a security model that more effectively adapts to the complexity of the modern environment, embraces the mobile workforce, and protects people, devices, apps, and data wherever they are located	--
Eu.Sec.265	Info	Implications <ul style="list-style-type: none">Trust is not granted until the user, system, or component can be authenticated and authorized first.Verify anything and everything trying to connect to its systems before granting access.Workforce: Authenticate users and continuously monitor and govern their access and privileges.Workloads: Enforce controls across the entire application stack, especially connections between containers or hypervisors in the public cloud.Data: Secure and manage data, categorize, and develop data classification schema, and encrypt data at rest and in transit.Supply Chain: Question and assess the integrity and security of suppliers and the delivered products, systems, and services.	--
Eu.Sec.266	Head	2.4.8 Least Privilege	
Eu.Sec.267	Info	Only grant the minimal set of permissions that are necessary for every operation or action - and no more	--

ID	Type	Requirement	Valid for
Eu.Sec.268	Info	Rationale Systems and users should operate while invoking as few privileges as possible. Granting permissions beyond the scope of the necessary rights of an action can allow a user or system to obtain or change information in unwanted ways. This principle limits the damage that can result from an attack, accident, or error. It also reduces the number of potential interactions among privileged systems to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.	--
Eu.Sec.269	Info	Implications <ul style="list-style-type: none"> Minimize the system elements to be trusted. This principle restricts how privileges are granted and revoked, and time out. 	--
Eu.Sec.270	Head	2.4.9 Usability & Manageability	
Eu.Sec.271	Info	Balance of security and usability - make secure behaviour easy instead of complex	--
Eu.Sec.272	Info	Rationale Make it easy to do the right thing, make it difficult to do the wrong thing, and make it almost impossible to do the catastrophic thing. Security controls should not obstruct users in performing their work and should not be difficult to manage. User interface must be easy to use, so that users routinely and automatically apply the mechanisms correctly. Relates to the paradigm of Least Astonishment in UI design and Simplicity Principles	--
Eu.Sec.273	Info	Implications <ul style="list-style-type: none"> A component or system should be designed to behave in a manner consistent with how users of that component are likely to expect it to behave. Design security interfaces and functions for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. 	--
Eu.Sec.274	Info	Note <ul style="list-style-type: none"> If security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security. 	--
Eu.Sec.275	Head	2.4.10 Design for Automation	
Eu.Sec.276	Info	Design for Automation to control complexity	--
Eu.Sec.277	Info	Rationale Manual security tasks are inefficient, expensive, and prone to inconsistencies and human error. It is no longer possible to deploy, operate, and secure complex applications and infrastructures without automation. Security, agility, scalability, and control are a direct function of automation in today's complex and rapidly changing technology and threat environment	--
Eu.Sec.278	Info	Implications <ul style="list-style-type: none"> Automation reduces complexity and ensures consistency. Reduces the talent gap by freeing scarce expertise from mundane tasks. Automated testing results in better components and software and reduces vulnerabilities and bugs. 	--
Eu.Sec.279	Head	2.4.11 Open Design	
Eu.Sec.280	Info	The security of a mechanism should not depend on the secrecy of the details of its design or implementation	--
Eu.Sec.281	Info	Rationale Assume outsiders and attackers will have access to source code (also for closed source software) and complete design and network topologies. Assume sensitive information regarding security measurements are leaked or sold. Encourage proactive reporting of security issues or vulnerabilities and act on such reports	--
Eu.Sec.282	Info	Implications <ul style="list-style-type: none"> Never store secrets in code, documentation, or configurations. Open security design promotes faster improvement cycles. Security measurements should be open and transparent. 	--
Eu.Sec.283	Info	Examples Shannon's Maxim: The enemy knows the system	--
Eu.Sec.284	Head	2.5 Process definition	
Eu.Sec.285	Info	To analyse the risks in the EULYNX architecture and define mitigating measures the Security Guideline of EUG, RCA, OCORA and EULYNX is used (available on the EUG website). 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 is to be updated regularly according to current status of threats and vulnerabilities as a life-cycle-management task.	--

ID	Type	Requirement	Valid for
Eu.Sec.286	Info	The process defined in the 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.287	Info	To set basic assumptions on possible attack vectors, an attacker type is defined. Furthermore, based on threats mapped to foundational requirements defined in IEC 62443 and an evaluation of the capabilities and resources required for these attacks, a security level can be defined for each zone.	--
Eu.Sec.288	Info	As part of the risk assessment based on a predefined target security level the risk can be analysed based on the exposure and vulnerability as well as the likelihood of a threat. Measures based on the IEC 62443 and new compensating measures can or have to be defined depending on the delta between current and target risk. This process is documented in detail to allow later adjustments.	--
Eu.Sec.289	Info	The operational process for analysing threats and risks to derive the suitable measures is defined and explained with an example in the Security Guideline.	--
Eu.Sec.290	Info	The process is supported by an Excel tool – ERORAT – see the EULYNX Security Threat and Risk Analysis [Eu.Doc.116].	--
Eu.Sec.619	Head	2.6 Constraints in Standards for Safety and Security	
Eu.Sec.649	Info	Standards for Safety and Security See Figure 1 on page 31.	--
Eu.Sec.621	Info	Figure in Eu.Sec.649 displays the relationship of Safety and Security in the design and specification processes of phases 1 to 5 according to CENELEC. The safety analysis leads to safety requirements and a safety case, whereas the security analysis leads to security requirements and a security case. The figure in Eu.Sec.649 shows that the security case proofs to the safety case the handling of adequate security measures to protect the overall system under consideration. Further it is shown that the security analysis can have an impact on the safety system design. It is also shown that mainly static (most likely not to be changed) requirements can be transferred to the safety side. Dynamic (changed regularly) requirements should be integrated to the system in a way, they are not directly related to safety approval.	--
Eu.Sec.622	Info	The EULYNX Security documentation provides input for the Security Case, required by TS 50701 for System Under Consideration definition, Threat and Risk analysis with SL-T and Definition of Measures (Security Specification)	--
Eu.Sec.291	Head	2.7 Assumption on available or to be established security services	
Eu.Sec.292	Info	In the following chapters security services that are necessary to allow security of life cycle are briefly introduced. They are not specified in detail, since it is assumed that they are already available or are to be established. Furthermore, there is suitable standards available how to design and implement them, so they are not EULYNX specific. As the organisational structure has to fit the size of the IM, the major security tasks might be handled by the SOC and expanded by additional units optionally.	--
Eu.Sec.293	Head	2.7.1 Security Operations Centre (SOC)	
Eu.Sec.294	Info	The Security Operations Centre (SOC) is the central organisational unit which monitors and analyses security-related information of the network. Furthermore, the personnel of the SOC are responsible to mitigate the risks of current vulnerabilities and to solve emerging security incidents.	--
Eu.Sec.295	Info	The SOC staff is formed by experts in the fields of vulnerability and security analysis. They are responsible for the evaluation of vulnerabilities as well as the detection of possible attack vectors. Hence one task of the SOC is to prevent future incidents and provide the coordination of mitigating measures. In addition, the SOC ensures the evaluation of real-time information from amongst others the SIEM and the handling of the resulting security incidents.	--
Eu.Sec.296	Info	Information about the current security situation and possible risks are gathered in reports available to the management level by the SOC personnel.	--
Eu.Sec.297	Info	The SOC may be supported with information and data provided by a European exchange platform. Furthermore, incidents which cannot be solved in the SOC can be transferred to the SIC/CSIRT.	--
Eu.Sec.298	Info	The IM may define which incidents are regarded and handled as security incidents.	--
Eu.Sec.299	Info	The core tasks of the SOC are: <ul style="list-style-type: none"> Identify: <ul style="list-style-type: none"> Ongoing analyses of the threat situation [Identify] Identification of weaknesses in IT security and their mitigation [Identify] Protect: <ul style="list-style-type: none"> Alerting for detected attacks and threats Defence / counter measures to limit the damage of cyber attacks [Protect] Reporting & Monitoring Advice Detect: <ul style="list-style-type: none"> Proactive monitoring of all IT systems, including self managed IT and Operational Technology (OT) [Detect] Respond: 	--

ID	Type	Requirement	Valid for
		<ul style="list-style-type: none"> Processing of incidents handled by 1st and 2nd level support and forwarded to the CSIRT for 3rd level support [Respond&Recover] Technical support for all security-related issues Recover: <ul style="list-style-type: none"> Processing of incidents handled by 1st and 2nd level support and forwarded to the CSIRT for 3rd level support 	
Eu.Sec.300	Head	2.7.2 Security Incident and Event Management (SIEM)	
Eu.Sec.301	Info	A Security Incident and Event Management (SIEM) is used to aggregate data from multiple sources and perform security related analysis. The analysis is used to detect security events like unauthorised connections to the network, unauthorised use of systems, vulnerabilities of systems, as well as attacks and indicators for attacks.	--
Eu.Sec.302	Info	As multiple data sources have to be connected to the SIEM and a wide range of information is gathered, a major task of the SIEM is to consolidate and correlate this data. Based on correlation rules multiple different events can be categorized and combined to meaningful security information. This set of information is analysed based on policies which define the behaviour of the monitored systems. Thus, both the normal state of the network and exceptions that should be classified as security incidents can be modelled.	--
Eu.Sec.303	Info	To allow immediate reactions based on the notifications provided by the SIEM, the logging capabilities of devices in the monitored network need to provide log data in real time to the SIEM system. These notifications are evaluated, and reactions are planned by the personnel of the Security Operations Centre (SOC).	--
Eu.Sec.304	Head	2.7.3 Security Incident Centre (SIC)	
Eu.Sec.305	Info	The Security Incident Centre requires the Security Information and Event Management (SIEM). This enables SIC staff to process the different information and put it into context. The initial reaction is carried out within the shortest possible time according to pre-designed playbooks, however considering implications on railway operation. The latter is done together with counterparts in Railway Operations Centre (ROC) and Railway Incident Centre (RIC). Any incident not handled by a dedicated pre-defined procedure must be individually assessed by a team of experts. Implication to railway operation must be assessed and reported based on expected effect of the incident. Appropriate measure must then be found, their implementation organised and orchestrated and the result monitored.	--
Eu.Sec.306	Info	The success of a SIC is based on three fundamental pillars: technologies, processes and trained employees. In addition, the cooperation of different companies is becoming increasingly important. Information exchange with others is key, e.g. with ISACs, on newly discovered vulnerabilities, attackers' procedures and their tools are an important part.	--
Eu.Sec.172	Head	2.7.4 Cyber security incident response team (CSIRT)	
Eu.Sec.173	Info	The CSIRT (Cyber Security Incidence Response Team) is responsible for handling actual security incidents, which don't follow the playbooks from 1st level support or the response from the 2nd level support of the Security Operations Centre (SOC).	--
Eu.Sec.199	Info	A CSIRT is not necessarily needed within the company and might be used as an external service. This is different from the SOC and its Security Incident and Event Management (SIEM) itself, due to the railway specific and confidential data.	--
Eu.Sec.200	Info	In both cases – internal and external CSIRT – a clear concept of data sharing, activation threshold or incident category and capabilities between SOC and CSIRT as well as access rights need to be clarified beforehand.	--
Eu.Sec.174	Head	2.7.5 Information Sharing and Analysis Centre (ISAC)	
Eu.Sec.175	Info	Security Operations need up to date information for threat intelligence. This enables the security team to constantly develop the use cases, following the current potential threat monitor.	--
Eu.Sec.202	Info	The ISAC can be widely used to share information in the circle of railway companies, meaning infrastructure and rolling stock. The information stays in a closed community but every railway company can get use out of the experience from everyone.	--
Eu.Sec.307	Head	2.8 Conformity to standard IEC 62443	
Eu.Sec.308	Info	The conformity to and implementation of IEC 62443-4-1, -4-2, -3-3, -2-4 is assumed.	--
Eu.Sec.310	Head	2.9 Information Security Management System	
Eu.Sec.311	Info	It is assumed that an Information Security Management System (ISMS) with a corresponding risk management is implemented and applied to operation technology for railway operation.	--
Eu.Sec.66	Head	3 Analyses	
Eu.Sec.67	Head	3.1 Assumptions / General requirements	
Eu.Sec.68	Info	For the EULYNX system the following assumptions are implied:	--

ID	Type	Requirement	Valid for
Eu.Sec.69	Info	<u>Access</u> It is assumed, that workstations, sensitive data and equipment are located in an access protected room or facility.	--
Eu.Sec.70	Info	<u>Physical Protection</u> It is assumed, that core security components have also a barrier of physical protection applied.	--
Eu.Sec.71	Info	<u>Installation</u> It is assumed, that the system has been properly tested and installed in a way that does not compromise the security of the system.	--
Eu.Sec.72	Info	<u>Operator</u> It is assumed, that operating personnel has been trained for usage with the system and is aware of secure operation principles. Issued policies are followed by the operators.	--
Eu.Sec.73	Info	<u>EN 50159</u> It is assumed, that systems in this context can handle hazards and events that are subject to [EN 50159] category 1 and category 2 networks. Which means that safety mechanisms are in place on communication links.	--
Eu.Sec.74	Info	<u>Security Policy</u> It is assumed, that the organisation enforces a security policy for organisation and personal requirements, e.g. according to [ISO 27001] or 62443-2-1.	--
Eu.Sec.312	Info	<u>NON-EULYNX devices in category 3 networks</u> It is assumed, that in category 3 networks many non-authorized devices exist and interference is expected. Measures to protect the EULYNX functionalities have to be defined and implemented. In contrast to category 1 or 2 networks, the behaviour of the other devices is not known. As a result, the focus must be set on process resilience against connection loss and degraded quality of service parameters like bandwidth, packet jitter, delay, packet loss.	--
Eu.Sec.193	Info	<u>Human Factors</u> It is assumed, that measures have been installed to avoid undetected manipulation at the security system to get network access by humans that got access to the physically secured systems.	--
Eu.Sec.316	Info	<u>RAMS and security</u> It is assumed, that RAMS (reliability, availability, maintainability, safety) aspects need to be considered separately.	--
Eu.Sec.317	Head	3.2 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. 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. Note: Security zones are not automatically networks.	--
Eu.Sec.319	Info	The resulting SuC with its initial zones is displayed below.	--

ID	Type	Requirement	Valid for
Eu.Sec.320	Info	<p>SuC (System under consideration) definition of the EULYNX risk assessments</p> <p>Legend:</p> <ul style="list-style-type: none"> Not specified in EULYNX EULYNX Not covered by risk assessment Logical connection 	--
Eu.Sec.321	Info	<p>To provide the basis for a structured risk assessment several different scopes have been defined. These are called SuC (System under consideration) and are linked to each other based on logical connections. Hence details of conduits or interfaces are not considered in the general overview shown in the figure in Eu.Sec.320. In this figure SuCs specified in the EULYNX standard are marked purple. Some of the SuCs are not defined in the EULYNX standard, they are surrounded by a solid black line. If a SuC is not part of the scope of this overall risk assessment, it is marked with a red and white striped background. Logical connections are shown with a solid black line. Every SuC is analysed individually. Most systems rely on a connection via the SCS (Subsystem Communication System) which is symbolized by a cloud in the middle. The figure does not specify a location for the systems. Due to decision in EULYNX the ILS-adapter must be located at the adjacent (legacy) EIL.</p>	--
Eu.Sec.322	Info	If assumptions do not fit the systems used, the threat and risk analysis might not be valid.	--
Eu.Sec.324	Info	The threat and risk analysis may be expanded and tailored to the IM's needs. As a result, measures might be reviewed as well.	--
Eu.Sec.325	Info	Basic assumptions that form the foundation for the risk analysis are presented below for each SuC. Implementation-specific risks are not analysed in the EULYNX security concepts.	--
Eu.Sec.326	Head	3.2.1 Electronic Interlocking (EIL)	
Eu.Sec.327	Info	The Electronic Interlocking (EIL) is the central system of the EULYNX-architecture. It is a communication participant for all SCI interfaces and is specified in EULYNX. It is assumed that the interlocking is located in a computer centre type of building.	--
Eu.Sec.328	Head	3.2.2 EULYNX field element Subsystems (EfeS)	

ID	Type	Requirement	Valid for
Eu.Sec.329	Info	The EfeS provides the link between EIL and Trackside Asset (TA, 3.2.4). It represents the boundary between EULYNX-scope and vendor-specific standards for the TA. Thus, it is specified in EULYNX. It provides interfaces for the control of field element subsystems for points, light signal, level crossings, etc. The EfeS is expected to be located in cabinets, containers or technical rooms which provide basic physical protection. Physical damage of the EfeS has to be detected by the EIL (assumed that the EfeS detects the damage, gets into "safe" state and disconnects from the EIL – other procedure using degraded mode possible). In this case the safety of the overall system is not affected.	--
Eu.Sec.330	Info	The EfeS can either be built as a Single-EfeS, connecting only one TA to the EIL, or as a Multi-EfeS, providing multiple communication endpoints for trackside assets in one device. The structure of a Multi EfeS is not covered in this risk assessment as the security highly depends on implementation and structure of the system.	--
Eu.Sec.331	Info	Connections from the EfeS to the TA using the SCS or another network are not considered in the risk assessment.	--
Eu.Sec.332	Info	The connection to the TA is addressed in the TA risk assessment.	--
Eu.Sec.333	Head	3.2.3 Maintenance and Data Management (MDM)	
Eu.Sec.334	Info	The Maintenance and Data Management (MDM) is specified in EULYNX. It is connected to EULYNX field element Subsystems EfeS, the EIL and the ILS-Adapter. It is assumed that the interlocking is located in a computer centre type building.	--
Eu.Sec.374	Info	The service function Time synchronisation is defined in the Maintenance and data management specifications [Eu.Doc.18].	--
Eu.Sec.335	Head	3.2.4 Trackside Assets (TA)	
Eu.Sec.336	Info	The Trackside Asset (TA) is not part of the EULYNX specification, it is only addressed in the EULYNX risk assessment to allow for a complete analysis. TAs are e.g., points, light signals and level crossing. The TA and its control unit is normally located near the track without any perimeter protection.	--
Eu.Sec.338	Head	3.2.5 Traffic Control System (TCS)	
Eu.Sec.339	Info	The Traffic Control System (TCS) terminate the SCI-CC connection and is directly connected to the EIL via the SCS. TCS is converting EULYNX SCI-CC messages to TCS proprietary messages and is converting TCS proprietary command to EULYNX SCI-CC commands. This is done using TCS software, of which only the communication interface is analysed in this risk assessment. The TCS itself is not subject of this assessment, but the interface to the TCS is analysed. SCI-CC uses RaSTA as safety protocol.	--
Eu.Sec.340	Head	3.2.6 ILS-Adapter	
Eu.Sec.341	Info	The ILS-Adapter is used to connect a EULYNX EIL to a legacy interlocking. If two EULYNX EILs are connected, no adapter has to be used as both speak SCI-ILS. The SCI-ILS connection is used to perform a safe handover of a train from one to another interlocking. This is usually performed using a shared block which is used to safely control pre-set routes across interlocking boundaries. The adapter is connected to the EIL via the SCS. It converts the EULYNX messages into a vendor specific data stream or an analogue signal of a vendor dependent bus system. It is assumed that the adapter is located in a room of the interlocking building. If the adapter is located in another facility a similar protection has to be provided.	--
Eu.Sec.342	Head	3.2.7 Maintenance User Interface (MaintUI)	
Eu.Sec.343	Info	The Maintenance User Interface (MaintUI) is used by the maintenance personnel. It is specified in EULYNX as interface M. Supplier-specific interfaces are not specified by EULYNX. The user interfaces (MaintUI device, e.g., laptop) is not covered in an own risk assessment, but the interface of the connected EULYNX component is addressed in the components risk assessment. MaintUI is expected to use SSH connections or proprietary protocols.	--
Eu.Sec.344	Head	3.2.8 Operational User Interface (OpUI)	
Eu.Sec.345	Info	The Operational User Interface (OpUI) is used by the operator of the Interlocking. It is not specified in EULYNX. The OpUI is assumed to be directly connected to the TCS. The EULYNX risk assessment does not cover OpUI.	--
Eu.Sec.346	Head	3.2.9 ETCS Radio Block Centre (RBC)	
Eu.Sec.347	Info	The Radio Block Centre (RBC) converts information sent from the EIL into an ETCS communication to the trains and vice versa. It terminates the SCI-RBC connection and is directly connected to the EIL and the TCS via the SCS. The RBC is converting EULYNX SCI-CC messages to RBC proprietary messages and is converting RBC proprietary command to EULYNX SCI-CC commands . ETCS and the RBC itself is not subject of this assessment, but the interface to the RBC is analysed. SCI-RBC uses RaSTA as safety protocol.	--
Eu.Sec.616	Info	The Centralised L1 Controller has not been assessed in the risk analysis and is not addressed in the measures definitions of Eu.Doc.114. The risk analysis of the RBC and corresponding measures can provide a basis for the of the Centralised L1 Controller.	--
Eu.Sec.348	Head	3.2.10 Adjacent (legacy) EIL	
Eu.Sec.349	Info	The adjacent legacy EIL is an interlocking which is not built based on EULYNX specifications. It is connected to EULYNX EILs via the SCI-ILS adapter. Only this adapter is addressed in a risk assessment of this security concept.	--

ID	Type	Requirement	Valid for
Eu.Sec.350	Head	3.2.11 Subsystem Communication System (SCS)	
Eu.Sec.351	Info	The Subsystem Communication System (SCS) is the central communication network used by the EULYNX systems. It is considered to be a Wide Area Network (WAN) and can be categorized as Cat 1 – 3.	--
Eu.Sec.352	Head	3.3 Threat and Risk analysis	
Eu.Sec.353	Info	The threat and risk analysis was performed based on architecture, concepts and procedures documented in this document, e.g. ERORAT (2.5). The documentation is available in the EULYNX Security Threat and Risk Analysis [Eu.Doc.116] as an editable Excel table to provide the ability to adjust risk assumptions, explanations and measures if needed for individualization or over the life-time.	--
Eu.Sec.354	Info	The results of the risk and threat analysis are the measures which are documented in the EULYNX Security Specification [Eu.Doc.114].	--
Eu.Sec.355	Head	4 Security Architecture	
Eu.Sec.356	Head	4.1 Technical architecture and interfaces	
Eu.Sec.357	Info	The technical architecture for security is based on the architecture for EULYNX, referenced in Chapter 2.	--
Eu.Sec.359	Info	The figure in Eu.Sec.362 shows the system under consideration with the security services (red) and supportive services (blue) added.	--
Eu.Sec.362	Info	<p>Architectural overview with security and supportive services</p> <p>Legend:</p> <ul style="list-style-type: none"> Not specified in EULYNX EULYNX Security Services Supportive Services Logical connection 	--

ID	Type	Requirement	Valid for
Eu.Sec.364	Info	In the following chapters all standard interfaces and systems (shown in Eu.Sec.362) are in scope of the security definitions and treated separately, if needed to meet the different requirements from the perspective of the security targets. These standard interfaces are: <ul style="list-style-type: none"> • SCI – defined in [Eu.Doc.92] • SMI – defined in [Eu.Doc.76] • SDI – defined in [Eu.Doc.77] • SSI – defined in [Eu.Doc.117] 	--
Eu.Sec.365	Head	4.1.1 SSI Standard Security Interfaces	
Eu.Sec.367	Info	Access to Security Services Platform is grouped on logical level with the Standard Security Interface (SSI), documented in detail in the Interface definition and specification SSI [Eu.Doc.117].	--
Eu.Sec.368	Info	The Security Services Platform has multiple sub-services, at least one for each security service.	--
Eu.Sec.369	Info	Security requirements for all subservices of the Standard Security Interface are given in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.Sec.366	Head	4.1.2 Security Services Platform (SSP)	
Eu.Sec.370	Info	The security services are available for every EULYNX device.	--
Eu.Sec.371	Info	The security services are briefly described in the following sections.	--
Eu.Sec.376	Head	4.1.2.1 Security Incident Detection	
Eu.Sec.623	Head	4.1.2.1.1 Security Logging Service	
Eu.Sec.377	Info	The Security Logging service is the data storage for all security related log and monitoring information. It stores the data and provides data to systems entitled to use them based on the IAM service. It ensures confidentiality, integrity, availability and non-repudiation of the data received. The service is able to fulfil real-time or near-real-time requirements e.g. required by SIEM services	--
Eu.Sec.389	Head	4.1.2.1.2 SIEM	
Eu.Sec.388	Info	The SIEM service provides security related monitoring of the system and supports the management of security incidents. The SIEM provides analytical functionality to detect security anomalies.	--
Eu.Sec.390	Info	The basis for the SIEM analytics can be the information of IDS, Security Logging and all information available from the diagnostic collector. Furthermore, the SIEM can be connected, amongst others, to the Asset inventory, the IAM and further services than can support the correlation process for analytics.	--
Eu.Sec.391	Info	If a potential anomaly is detected, an alarm is issued to relevant organizational units. Data provided by a Network Intrusion Detection (IDS) can be used as an additional input to the SIEM.	--
Eu.Sec.392	Info	The SIEM service is a mainly technical service, however heavily interconnected to different data sources and may include additional non-technical procedures to enhance or verify anomaly detection. These non-technical procedures have interfaces to units operating Command Control Signalling system, units operating the network and units controlling and operating the railway service itself. This service is expected to change constantly over time to keep up with threat intelligence.	--
Eu.Sec.393	Info	The SIEM service provides the following functionality: <ul style="list-style-type: none"> • analytical functionalities to detect potential security incidents • alarming functionality to trigger human action • auto-react functionality to trigger other technical systems • ticket system to manage incidents and events 	--
Eu.Sec.379	Head	4.1.2.2 Backup	
Eu.Sec.380	Info	The Backup service offers backup services to store relevant information in a secure way ensuring confidentiality, integrity and availability for restore. This service processes only data files provided by the device doing the backup. The backup service orchestrates the backups, hence it triggers backup processes at the target and monitors the success of this backup. The service does not ensure that the backup's content is usable for restoring. The format of the file is depending on implementation of the backup generating system.	--
Eu.Sec.382	Head	4.1.2.3 Identity and Access Management (IAM)	
Eu.Sec.383	Info	The Identity and Access Management service provides identity management for personnel interacting with machines. The accuracy and reliability of identifying an entity is of paramount importance. This identification procedure must be secure. Based on roles assigned to these identities, access management information is generated and provided to subsystems. The roles define the rights granted. The rights include for example granting communication setup or use of a functionality or capability of a subsystem/device.	--
Eu.Sec.385	Head	4.1.2.4 Public Key Infrastructure (PKI)	

ID	Type	Requirement	Valid for
Eu.Sec.386	Info	The Public Key Infrastructure service provides the digital representation of the identity of an entity in the form of certificates used for public-key cryptography (encryption and integrity protection). It provides technical services to handle request, renew, revoke and validate certificates. To fulfil its purpose, it requires the identity management part of the IAM. This can be provided by the IAM service or by non-technical procedures/processes ensuring the management of the identify. This service is only having interfaces to technical systems if the IAM service is present. If the IAM service is not present, this service shall implement the identity management part of the IAM service or rely on external identity management.	--
Eu.Sec.397	Head	4.1.3 Shared Supportive Services	
Eu.Sec.398	Info	The supportive services are briefly described in the following sections.	--
Eu.Sec.399	Head	4.1.3.1 Asset Inventory	
Eu.Sec.400	Info	The asset inventory is part of the asset management process. The asset management is used to track the lifecycle of all hardware and software assets. The assets managed include all assets relevant within the EULYNX architecture and not only the security related assets. It tracks the data of assets beginning with the interface from the procurement management, ending with the decommissioning. This service is interconnected with commercial processes, including supply chain and procurement processes.	--
Eu.Sec.401	Info	The asset management contains amongst others: <ul style="list-style-type: none"> • Asset Inventory • Configuration Management System (CMS) • Maintenance aspects • Commercial aspects 	--
Eu.Sec.402	Info	For use within EULYNX, the CMS is relevant for the Software (configuration and software) management process. The CMS manages the software and configuration of the assets in the context of a desired overall state. This service is sometimes referred as Configuration Management Database (CMDB). It must provide a versioning system which records and provides the configuration used by the assets. The CMS does not store software or configurations. The software and configuration is stored in the SW+Config Repository.	--
Eu.Sec.403	Info	The CMS orchestrates configuration updates using the SW+Config Repository service to deploy software files and configuration.	--
Eu.Sec.404	Info	The EULYNX subsystem MDM is supporting this task by performing a lookup for the software and configuration version defined in the CMS. Afterwards it is requesting the corresponding software and configuration from the SW+Config Repository. This software and configuration are then deployed to the asset. This service is a technical service interconnected to the life-cycle-management of the asset and the system, as well as with data preparation procedures. This service supports keeping the overall system in a certified state. The process is displayed in the figure in Eu.Sec.411.	--
Eu.Sec.405	Info	There are additional processes required around this update procedure to ensure smooth operation. The interlocking for example should set asset into maintenance mode. Since all these processes can be IM and supplier specific, they are not specified in more detail.	--
Eu.Sec.406	Info	Asset inventory includes attributes to each asset giving indication on their position and function in the logical architecture (e.g. to be used for risk inheritance during risk management process) and physical architecture (e.g. to be used for updates, retro-fit efforts).	--
Eu.Sec.407	Info	The asset inventory provides the following connectivity and support interaction: <ul style="list-style-type: none"> • Interacts with Life-Cycle Managers • Interacts with maintenance personnel (maintenance, replacement) • Interacts with build projects (import/create assets to be managed) • Interacts with IAM (basic data for identity, decommissioning of asset) • Supports maintenance activities • Provides technical, commercial and supply chain data based on authentication and authorisation based on IAM service • Documents physical (e.g. location) and high-level logical (e.g. EIL area) context of asset • Provides Configuration Management System (CMS) orchestrating software and configuration changes ensuring compliance with safety regulation/certificates • The Configuration Management System interacts with processes/systems supporting change • The Configuration Management System interacts with the MDM 	--
Eu.Sec.409	Head	4.1.3.2 Software and Configuration Repository	
Eu.Sec.410	Info	The software and configuration repository service is used by the MDM. The files can be accessed based on the IAM service.	--

ID	Type	Requirement	Valid for
Eu.Sec.411	Info	<p>SW and Config deployments process</p> <pre> graph LR Asset[Asset] -- "SW/Config update" --> MDM[MDM] MDM -- "Request" --> SW[SW + Config Repository] SW -- "Send" --> MDM MDM -- "Request for Asset" --> CMS[CMS] CMS -- "Gives status" --> MDM SW -- "Gives data" --> DP[Data Prep] DP -- "Request for Asset" --> CMS </pre>	--
Eu.Sec.416	Head	4.1.3.3 Diagnostics collector	
Eu.Sec.417	Info	The service function Diagnostics collector gathers all safety, non-safety and non-security-specific information distributed by the connected components related to diagnostic, monitoring and logging. This set of information can be used to investigate malfunctions and perform troubleshooting. These information can be forwarded to the SIEM to be a basis for a more profound investigation of security incidents, e.g., used by digital forensics.	--
Eu.Sec.419	Info	The service function Diagnostics collector is defined in the Maintenance and data management specifications [Eu.Doc.18].	--
Eu.Sec.423	Head	4.1.4 Zone Model	
Eu.Sec.424	Info	The zone model below covers all security related aspects from EULYNX. This zone model is designed according to TS 50701 and 62443-3-2.	--
Eu.Sec.425	Info	Zone Model See Figure 2 on page 32.	--
Eu.Sec.652	Info	Note: The SSI-connection to the Adjacent Interlocking System is not displayed in the System Architecture of Eu.Doc.7. The Security Concept is introducing the ILS-Adapter connected to SSP via SSI to ensure a secure connection to an Adjacent Interlocking System.	--
Eu.Sec.426	Info	The zone SCS represents multiple zones. Since for securing the communication (data in transit) through the communication system (SCS) it is not relevant how the communication system is set up in detail, the SCS is seen as one zone for the threat and risk analysis and security specification.	--
Eu.Sec.427	Info	The zone "Asset Management" represents the services linked to Asset Management process.	--
Eu.Sec.428	Info	The zone "Adjacent EIL" is used to illustrate the connection between EULYNX-compliant EILs. Connections of this zone to e.g. an EfeS or centralized services are not displayed.	--
Eu.Sec.437	Head	4.1.5 Securing Communication	
Eu.Sec.451	Head	4.1.5.1 Requirements for safety related communication	
Eu.Sec.196	Info	Requirements for safety-related communication over transmission systems like IP networks are defined in [EN 50159] for different categories of networks.	--
Eu.Sec.207	Info	From a safety perspective according to [EN 50159], no cryptographic measures are required within a category 1 and category 2 network.	--
Eu.Sec.208	Info	If a category 3 network is used, additional security measures are required. With these measures, a category 2 equivalent network or individual connection can be implemented on top of a category 3 network.	--
Eu.Sec.455	Info	From a security perspective, additional measure may be required depending on the chosen security level (IEC 62443-3-2).	--
Eu.Sec.458	Info	The EN 50159 states a classification of safety-related communication systems (see figure in Eu.Sec.501) that can be applied to non-safety or non-safety related as well. As a result, this classification can be used for all EULYNX communication (SCI, SMI, SDI, SSI) and applied in accordance with the security target.	--
Eu.Sec.459	Info	A non-cryptographic safety code only protects against technical failures according to EN 50159. By using a cryptographic safety code the data is protected against intentional manipulation and attacks.	--

ID	Type	Requirement	Valid for
Eu.Sec.460	Info	Following the definitions of EN 50159, RaSTA uses the non-cryptographic safety code MD4 to protect against message corruption. Based on cryptographic analysis MD4 is considered deprecated for security purposes.	--
Eu.Sec.501	Info	<p>Figure C.1 from EN 50159:2010</p> <p>Figure C.1 – Classification of the safety-related communication system</p>	--
Eu.Sec.462	Info	<p>Following the definition from EN 50159, Figure C1, the following methodologies can be used to protect safety data in category 3 networks using the current protocol definitions within EULYNX:</p> <ul style="list-style-type: none"> • Application of cryptographic code + non cryptographic safety code (B1) • Application of encryption + non cryptographic safety code (B0) 	--
Eu.Sec.472	Head	4.1.5.2 Protection solutions / concepts (Variant A, B, C)	
Eu.Sec.473	Info	This chapter describes the basic concepts to protect communication when using category 3 networks according to EN 50159. These concepts are designed to be compliant with EN 50159 for safety and safety related. However, the concepts can be used for non-safety as well and can be applied to network with other categories than category 3.	--
Eu.Sec.474	Head	4.1.5.2.1 Basic concept of Variant A, B, C	
Eu.Sec.475	Info	The basic concepts are documented in this chapter, detailed requirements for all variants are specified in the EULYNX Security Specifications [Eu.Doc.114] and the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.Sec.476	Info	Requirements expected to change frequently or that might have to be changed fast due to major changes in threat landscape or vulnerability/exploit are documented in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.Sec.625	Info	It is recommended to the IM to define requirements regarding the desired and feasible update path for components.	--
Eu.Sec.479	Info	For category 3 networks (EN 50159) the variants A, B or C can be selected.	--
Eu.Sec.480	Info	For systems requiring protection for data in transit for integrity and/or confidentiality, according to a risk assessment, the variants A, B or C can be selected.	--

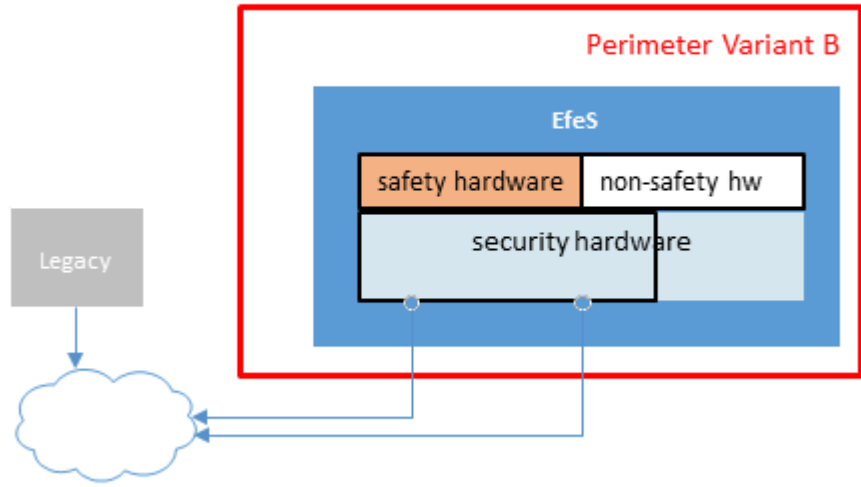
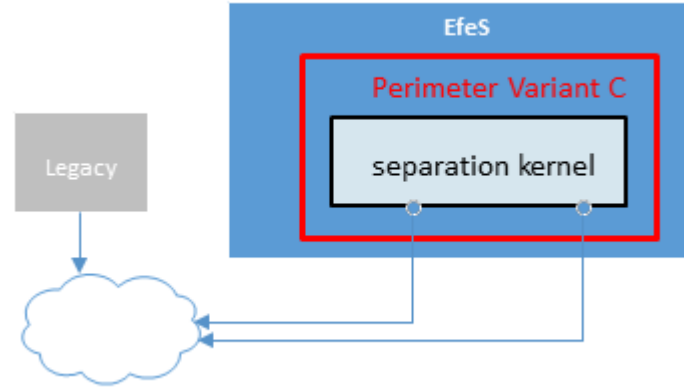
ID	Type	Requirement	Valid for
Eu.Sec.485	Info	Following Variants A, B and C are briefly introduced.	--
Eu.Sec.486	Info	"Variant A" ("Crypto Box") allows to encrypt the data in transit within additional components connected directly to the field element controller and central components. For this solution the separation principle in the figure in Eu.Sec.500 applies.	--
Eu.Sec.487	Info	"Variant B" integrates the network and encryption or integrity protection capability into the EULYNX field element Subsystem EfeS. Nevertheless, it is realized in different hardware modules within the same controller housing. That allows to follow the separation principle of the figure in Eu.Sec.500.	--
Eu.Sec.500	Info	<div>Separation of safety and security when implemented Security on Transport layer</div> <div><div><div>Safety Application using RaSTA</div></div><div>Safety</div><div></div><div><div><div>Security with cryptographic measures on Transport Layer</div><div>Transport Protocol, e.g. TCP</div><div>Network Transmission via Network of cat. 1, 2 or 3 after 50159</div><div>Cable and Connector</div></div><div>Network and Security</div></div></div>	--
Eu.Sec.489	Info	"Variant C" integrates security and safety functionalities in the same hardware component. Both are using software-based separation. Variant C follows the principle of the figure in Eu.Sec.490.	--

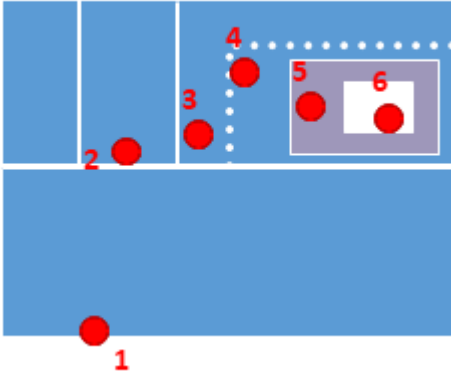
ID	Type	Requirement	Valid for
Eu.Sec.490	Info	<p>Separation of safety and security when implemented Security on Application layer (illustrative)</p>	--
Eu.Sec.491	Head	4.1.5.2.2 Variant A "Crypto Box"	
Eu.Sec.492	Info	Variant A system is implemented as network connected and dedicated components with their own device housings ("Crypto Box").	--

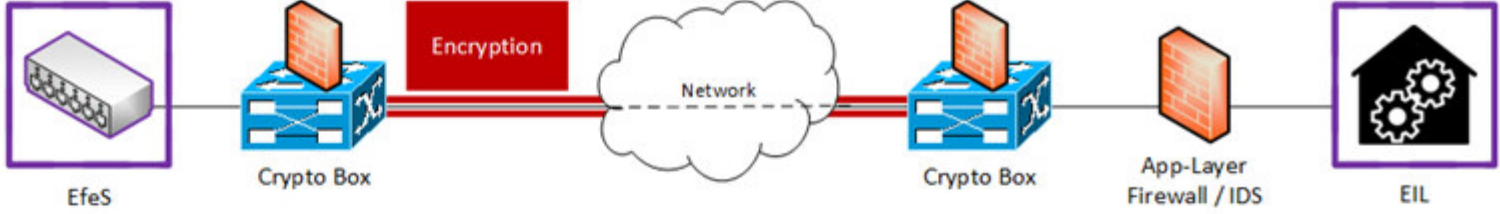
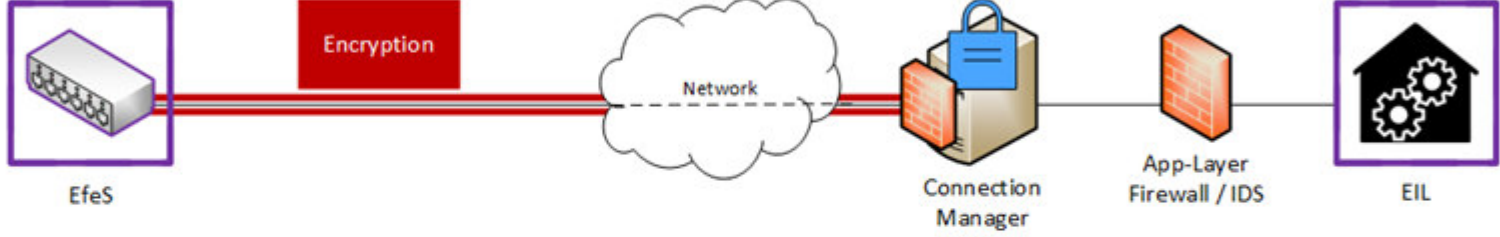
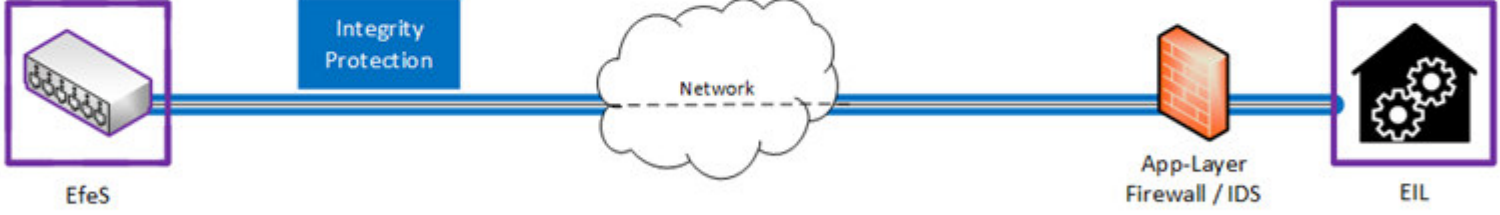
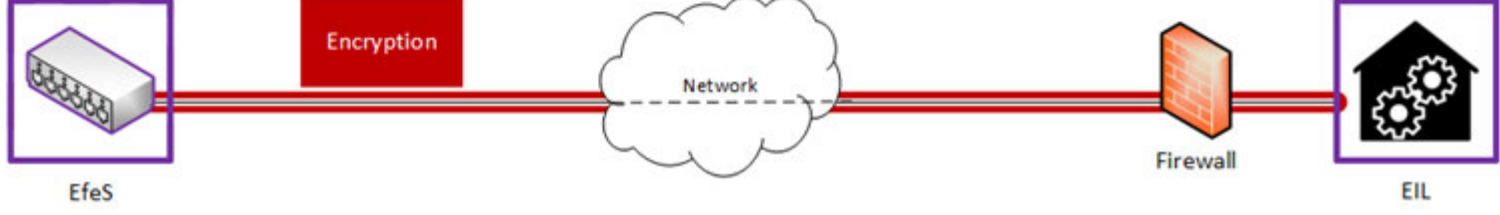
ID	Type	Requirement	Valid for
Eu.Sec.626	Info	The Crypto Box component is independent from any safety component or device.	--
Eu.Sec.627	Info	The Crypto Box components are implementing a secured virtual private network ensuring protection of integrity and confidentiality.	--
Eu.Sec.494	Info	If the IM is using Variant A, the IM needs to specify Variant A implementation in detail.	--
Eu.Sec.498	Info	For safety or safety-related traffic EN 50159 also applies to the network cabling connecting the Crypto Box and the EfeS. Measures are required to create a category 1 or category 2 network to fulfil the requirements of EN 50159.	--
Eu.Sec.502	Info	<p>Variant A: Crypto Box</p>	--
Eu.Sec.503	Head	4.1.5.2.3 Variant B and C common requirements	
Eu.Sec.504	Info	Variant B and C are implemented using TLS over TCP.	--
Eu.Sec.506	Head	4.1.5.2.4 Variant B specific requirement: "TLS with dedicated hardware board"	
Eu.Sec.507	Info	In Variant B, the separation between security and safety is done through dedicated hardware for security functionality.	--
Eu.Sec.628	Info	In Variant B, the dedicated hardware board used for the security functionality is replaceable.	--
Eu.Sec.629	Info	In Variant B, the safety certification is not integrating security into safety assurance.	--
Eu.Sec.630	Info	The separation principle is shown in Eu.Sec.513.	--
Eu.Sec.509	Info	The hardware board may offer offloading of cryptographic operations and secure key storage to other components (e.g., TPM, HSM).	--
Eu.Sec.510	Info	In case of required changes on this dedicated hardware board, assurance or re-certification may be limited to these changes leaving all other devices, e.g. safety devices, unchanged. This might reduce effort and shorten time for certification.	--
Eu.Sec.511	Info	In Variant B, the dedicated security hardware board is located in the same device housing as the SCI-XX part of the EULYNX field element Subsystem EfeS to ensure protection of cabling and hardware of the EULYNX field element Subsystem EfeS.	--

ID	Type	Requirement	Valid for
Eu.Sec.513	Info	<p>Variant B: "TLS with dedicated hardware board"</p> <p>The diagram illustrates the architecture for Variant B. At the top, an 'EIL' (red box) is connected to a 'TLS endpoint' (blue box). Below this, a 'Transport network element' (purple box) contains a 'NAC' (purple box) and an 'eth' (purple box). The 'NAC' is connected to the 'eth' box, which is also connected to a 'sec chip' (blue box). The 'sec chip' is connected to a 'field element Subsystem' (yellow box). Inside the 'field element Subsystem', there is a 'NAC' (blue box), 'IPv6' (purple box), 'TCP' (purple box), and 'TLS' (blue box). The 'NAC' is connected to the 'IPv6' box, which is connected to the 'TCP' box, which is connected to the 'TLS' box. The 'TLS' box is connected to the 'sec chip'. The 'field element Subsystem' is connected to a 'Trackside Asset' (purple box) which contains an 'e.g. drive' (black box). The 'field element Subsystem' is also connected to a 'safety subsystem' (red box) which contains 'RaSTA (safety)' (red box), 'e.g. safety point machine' (red box), and 'e.g. driver' (red box). The 'RaSTA (safety)' box is connected to the 'e.g. safety point machine' box, which is connected to the 'e.g. driver' box. The 'e.g. driver' box is connected to the 'e.g. drive' box.</p>	--
Eu.Sec.514	Head	4.1.5.2.5 Variant C specific requirement: "TLS with software separation"	
Eu.Sec.515	Info	Variant C is fully integrated on the same hardware, and separation is done on software level. This concept was developed for rail in the German national project Haselnuss and is well known from the aviation and automotive industry. A separation kernel (security element) provides separated environments for safety, non-safety and security applications. This way, the safety application can be secured and protected from changes, whilst the security part is regularly updated. This can be seen in the figure in Eu.Sec.521.	--
Eu.Sec.516	Info	In Variant C, the separation between security and safety is done at software level where sufficient separation of different tasks running on subsystems is ensured and approved.	--
Eu.Sec.631	Info	Certified or approved separation kernels or separation operating systems may be considered.	--
Eu.Sec.632	Info	The level of required separation might be adjusted by safety assurance/certification requirements.	--
Eu.Sec.517	Info	Software based security modules or trusted execution environments, or hardware security modules may be used within or as an extension of this concept.	--
Eu.Sec.518	Info	The software system may ensure separation from dedicated hardware as well.	--
Eu.Sec.520	Info	The separation approach may be integrated into safety assurance / certification structure enabling easy updates of hardware, firmware or software. This ensures fast re-certification in case of required security related changes and should not lead to a re-certification of the safety part.	--
Eu.Sec.633	Info	In Variant C, the safety certification is not integrating security into safety assurance.	--

ID	Type	Requirement	Valid for
Eu.Sec.521	Info	<p>Variant C "TLS with software separation"</p>	--
Eu.Sec.522	Head	4.1.5.2.6 Physical protection for Variants A, B, and C	
Eu.Sec.523	Info	It is assumed that physical protection is always required up to certain extend to support defense in depth concepts.	--
Eu.Sec.525	Head	4.1.5.2.6.1 Physical protection for Variant A	
Eu.Sec.527	Info	The perimeter for Variant A (Crypto Box): EULYNX field element Subsystem EfeS, Crypto Box and network equipment and cabling connecting both. If other devices are connected to the clear-text (unencrypted interfaces) side of the Crypto Box, these devices belong to the perimeter as well. This results in a perimeter which is usually the field element cabinet, the rack or a compartment of a room/container.	--
Eu.Sec.528	Info	<p>Perimeter for Variant A</p>	--
Eu.Sec.529	Head	4.1.5.2.6.2 Physical protection for Variant B	
Eu.Sec.526	Info	The perimeter for Variant B (TLS with dedicated hardware board): The dedicated hardware board is located inside the EULYNX field element Subsystem EfeS device (or blade sliding into the rack). The perimeter is therefore this device housing if the hardware board is not directly accessible from outside of the device housing (Eu.Doc.114, M00002).	--


ID	Type	Requirement	Valid for
Eu.Sec.530	Info	<p>Perimeter for Variant B</p> 	--
Eu.Sec.531	Head	4.1.5.2.6.3 Physical protection for Variant C	
Eu.Sec.532	Info	The perimeter for Variant C (TLS with software separation): The perimeter of the combined safety and security device is the device housing.	--
Eu.Sec.533	Info	<p>Perimeter for Variant C</p> 	--
Eu.Sec.534	Head	4.1.5.2.6.4 Physical defence in depth	
Eu.Sec.535	Info	In a defence in depth concept for physical security, additional perimeters surrounding the innermost perimeter may be considered.	--
Eu.Sec.536	Info	The IM may consider to ensure basic physical access control to each perimeter where components are installed or stored.	--
Eu.Sec.634	Info	Illustrative perimeters are shown in figure in Eu.Sec.539 (1: House entrance, 2: Floor, 3: Room, 4: Cage, 5: Rack, 6: Device). This structure applies as well for container and cabinet.	--
Eu.Sec.537	Info	If authorisation is required for physical access, the IM may ensure that the physical access protection elements (e.g. locks) are connected to a physical access management and control system.	--

ID	Type	Requirement	Valid for
Eu.Sec.539	Info	<p>Physical security</p>  <p>The diagram shows a blue rectangular area divided into several sections. A red dot labeled '1' is at the bottom left. A red dot labeled '2' is in the top left section. A red dot labeled '3' is in the top middle section. A red dot labeled '4' is in the top right section. A red dot labeled '5' is in the top right section, inside a white square. A red dot labeled '6' is in the top right section, inside a white square.</p>	--
Eu.Sec.540	Head	4.1.5.2.7 Connection Manager	
Eu.Sec.541	Info	<p>The connection manager provides multiple security related features.</p> <ol style="list-style-type: none">1. Support of migration or coexistence of different variants and of different releases concerning security over the time.2. Terminating TLS connection at a defined point, either to off-load TLS load from EIL or to monitor encrypted network traffic.	--
Eu.Sec.636	Info	<p>From a non-security point of view, the connection manager may offer abilities to support migration or coexistence of different SCI/PDI versions, offloading this task from the EIL. It may support as well using non-EULYNX devices during migration to a pure EULYNX environment.</p>	--
Eu.Sec.542	Info	<p>The network between the connection manager and the EIL core can be cat.2 (RaSTA over UDP) or cat.3 (RaSTA over TLS/TCP), depending on connection manager's implementation and risk assessment.</p>	--
Eu.Sec.543	Info	<p>There is no impact to the system architecture, as the connection manager is part of the EULYNX Subsystem EIL. The risk assessment and the measures do not include details of a connection manager implementation.</p>	--
Eu.Sec.544	Head	4.1.5.2.8 Reference points	
Eu.Sec.545	Info	<p>To have a common understanding when discussing different setups, the EULYNX Network Guideline (Eu.Doc.25) provides reference point definitions.</p>	--
Eu.Sec.553	Head	4.1.5.3 Communication models and migration	
Eu.Sec.554	Info	<p>In the following figure in Eu.Sec.556 the different communication models to protect communication via networks are displayed. The shown EULYNX field element Subsystem EfeS is used as an example. There are all EULYNX endpoints possible.</p>	--
Eu.Sec.555	Info	<p>The different models in the figure in Eu.Sec.556 can be applied in cat 2 and cat 3 networks.</p>	--

ID	Type	Requirement	Valid for
Eu.Sec.556	Info	<p>Communication models</p> <p>Variant A IPSec with encryption</p>  <p>Variant B & C (1) TLS 1.3 without integrity protection only cipher</p>  <p>Variant B & C (2) TLS 1.3 with integrity protection only cipher</p>  <p>Variant B & C (3) TLS 1.3 with encryption</p> 	--
Eu.Sec.557	Info	The figure in Eu.Sec.556 uses the communication of EULYNX field element Subsystems EfeS to the Interlocking (EIL) as an example to show the different alternatives for the protection of integrity and confidentiality.	--
Eu.Sec.558	Info	Variant A is based on the Crypto Box to encrypt the traffic in the network (SCS). The encryption tunnel is used by several different endpoints on client and on server-side. Hence it does not implement end-to-end and does not implement mutual authenticated security.	--
Eu.Sec.559	Info	Variant B and C are more diverse. Both rely on the integration of TLS in the EfeS. The integration can be implemented using a separate security component at the EfeS (Variant B) or using integrated security mechanisms which are separated from the safety using separation kernels (Variant C). As Variant B and C provide end-to-end and mutual authenticated security the security mechanism can be chosen based on the requirements for the interface or connections. Setup 1 provides security from the entity to the Connection Manager, which is terminating the TLS connection. Thus, the unencrypted traffic is visible to e.g., the application layer firewall, and IDS or juridical recording devices. Furthermore, the Connection Manager might provide a simplified update path, as shown in the figure in Eu.Sec.561. Setup 2 uses TLS integrity only protection. This allows to analyse the traffic in all parts of the network. Mutual authentication with the entity on EIL-side is possible in this case. Setup 3 is working in the same way as Setup 2, but with enabled encryption. In this scenario it is not possible to analyse the unencrypted traffic for intermediate entities so the endpoint (EIL) needs to provide the capability to provide juridical recording and security logging avoiding non-intrusiveness (as defined in EN 50126) to safety.	--

ID	Type	Requirement	Valid for
Eu.Sec.561	Info	<p>Migration path for the communication models</p> <p>The diagram illustrates four communication variants between an EfeS (End-to-End Firewall/Encryption Server) and an EIL (End-to-End Intrusion Detection/Logging) component, connected via a Network cloud.</p> <ul style="list-style-type: none"> Variant A: IPSec with encryption - Traffic flows from EfeS through a Crypto Box (Encryption) to the Network, then through another Crypto Box to the EIL. A dashed line also connects the two Crypto Boxes. Variant B & C (1): TLS 1.3 without integrity protection only cipher - Traffic flows from EfeS through Encryption to the Network, then through a Connection Manager to the EIL. Variant B & C (2): TLS 1.3 with integrity protection only cipher - Traffic flows from EfeS through Integrity Protection to the Network, then through an App-Layer Firewall / IDS to the EIL. Variant B & C (3): TLS 1.3 with encryption - Traffic flows from EfeS through Encryption to the Network, then through an App-Layer Firewall / IDS to the EIL. 	--
Eu.Sec.562	Info	<p>As not all EULYNX systems might be designed with just one consistent Variant, a migration path for the different communication models is necessary. The figure in Eu.Sec.561 shows a possible implementation of different communication models in one EULYNX network. Again, only the EfeS to EIL connection is used as an example. Variant A and setup 1 of Variant B & C both use an encryption termination device. At the Crypto Box the encryption tunnel and on the Connection Manager separate TLS connections are terminated. Both unencrypted connections are forwarded to the security components like Firewalls or Intrusion Detection Systems (IDS). Furthermore, it's possible to directly forward the Crypto Box traffic to the Connection Manager. Setups 2 and 3 are end-to-end secured connection and thus terminate on the EIL. This requires TLS functionality at the EIL. While setup 2 can be analysed by the same Firewall or IDS, setup 3 might require a different configuration or device as only the encrypted traffic can be analysed.</p>	--
Eu.Sec.637	Head	4.1.5.4 Security for PDI layer	
Eu.Sec.638	Info	<p>According to the System Architecture Specification (Eu.Doc.16) only SCI messages which have been received by the expected communication partner shall be processed. The check, if a packet can be treated, is supported by security. It is implemented in two different ways depending on which variant A, B or C is chosen.</p>	--
Eu.Sec.639	Info	<p>The check is performed based on the configuration and engineering data provided e.g. by the MDM. The data definition contains the processable combinations of identifiers used to identity the communication partner and the technical and operational identifiers of SCI-XX. These define the valid communication relations.</p>	--
Eu.Sec.640	Info	<p>If packets are not processed, the connection is closed and security logging messages are provided to the SSP. The process for allowing the component to reopen the connection is defined differently for EfeS and the EIL.</p>	--
Eu.Sec.641	Info	<p>The following identification mechanisms for communication partners are considered:</p>	--
Eu.Sec.642	Head	4.1.5.4.1 Variant A:	

ID	Type	Requirement	Valid for
Eu.Sec.643	Info	The communication partner is identified based on the remote IP address. Note: The authenticity of the remote IP address needs to be ensured by the Subsystem Communication System.	--
Eu.Sec.644	Head	4.1.5.4.2 Variant B and C:	
Eu.Sec.645	Info	The communication partner is identified based on the common name of the certificate used by the communication partner for establishing the TLS connection.	--
Eu.Sec.563	Head	4.2 Process architecture	
Eu.Sec.564	Info	As processual and organisational set is different from IM to IM, the following definitions will focus on generic process architecture to generate a common terms for communication in the EULYNX security domain.	--
Eu.Sec.565	Info	It is assumed that all management functionalities are structured, following ITIL. As ITIL focusses on processes rather than organization and technology, this structure eases the interoperability on process level between different internal organizational units or external service providers.	--
Eu.Sec.566	Info	Following the ITIL framework enables organisational changes and eases adaption of known processes of other companies following the same framework. It reduces time to on-board personnel as the terminology and interfaces between units are identical or similar to the previous job.	--
Eu.Sec.568	Info	The systemic relation between railway operation, command and control systems to operate the railway infrastructure, communication networks and security topics must be taken into account.	--
Eu.Sec.572	Info	The IM may setup processes and reports to answer the following questions: <ul style="list-style-type: none"> • Is railway operation safe given the current security incident or vulnerability? (yes – no) • Is there a current security incident or vulnerability affecting availability of railway operation? (yes – no) • Which railway lines are affected in terms of loss of safety due to current security incident or vulnerability? (List of railway infrastructure, lines, areas affected) • Which railway lines are affected in terms of railway operation availability due to current security incident or vulnerability? (List of railway infrastructure, lines, areas affected) 	--
Eu.Sec.573	Info	If required by authorities or legal requirements additional reports may be generated. Note: This should be part of the Information Security Management System. The final operational decision must be made by the railway operations manager or equivalent.	--
Eu.Sec.582	Info	Designing security for a complex system requires to consider organisational and procedural topics. To create a terminology useful to discuss solutions and to exchange experiences, an illustrative organisation is used to define names for roles or organisational units.	--
Eu.Sec.583	Info	Every infrastructure is managed (long term) and operated (short term) but management and operation are related to each other. The management covers strategic and preparative topics like life-cycle-management or procurement. The operations cover the daily business of keep it running and report failure/issues to the management part. These issues will then be integrated into strategic decisions or life-cycle-management like requiring error correction or patches.	--
Eu.Sec.588	Info	The procedural organisation as an overlay over the organisational structure implements the interfaces and interactions. As framework for the procedural setup, the ITILv3 framework may be used.	--
Eu.Sec.589	Info	As only the relevant and major parts of the ITILv3 framework shall be used, a selection is made with respect to managing the infrastructure and responding to security incidents. The selection is guided by: <ul style="list-style-type: none"> • What is required to keep track of the current state? • What is required to change the setup in a controlled manner? • What is required if something goes wrong (incident, problem)? • What is required to support safety certification and keep a certified state? (Test/Config) 	--
Eu.Sec.590	Info	The following figure shows the ITILv3 framework and the elements selected as relevant.	--

ID	Type	Requirement	Valid for
Eu.Sec.591	Info	<p>ITILv3 framework</p>  <p>The diagram illustrates the ITILv3 framework with five main processes arranged horizontally at the top. Below each main process, several sub-processes are listed in a vertical column. The sub-processes are color-coded to match their parent process: purple for Service Strategy, red for Service Design, blue for Service Transition, green for Service Operation, and yellow for Continuous Service Improvement.</p> <ul style="list-style-type: none"> Service Strategy (purple): Demand Mgt, Financial Mgt, Strategy Generation, Service Portfolio Mgt Service Design (red): Service Catalogue Mgt, Service Level Mgt, Capacity Mgt, Availability Mgt, IT Service Continuity Mgt, Information Security Mgt, Supplier Mgt Service Transition (blue): Knowledge Mgt, Change Mgt, Asset and Configuration Mgt, Release and Deployment Mgt, Transition Planning and Support, Service Validation and Testing, Change Evaluation Service Operation (green): Incident Mgt, Problem Mgt, Event Mgt, Request Fulfillment, Access Mgt, Operations Mgt, Service Desk, Application Mgt, Technical Mgt, IT Operations Mgt Continuous Service Improvement (yellow): Service Measurement, Service Reporting, Service Improvemnt 	--
Eu.Sec.592	Info	The following services shall be considered:	--
Eu.Sec.593	Info	<ul style="list-style-type: none"> • Service Design: <ul style="list-style-type: none"> • Information Security Management: for Security infrastructure • Supplier Management: for Security infrastructure • IT Service Continuity Management: for Security infrastructure • Availability Management • Capacity Management 	--
Eu.Sec.594	Info	<ul style="list-style-type: none"> • Service Transition: <ul style="list-style-type: none"> • Change Management • Service Asset and Configuration Management <ul style="list-style-type: none"> • Asset Inventory • Configuration Management • Identity Management • Release and Deployment Management • Service Validation and Testing • Change Evaluation • Transition Planning and Support 	--

ID	Type	Requirement	Valid for
Eu.Sec.595	Info	<ul style="list-style-type: none">• Service Operation<ul style="list-style-type: none">• IT Operation Management<ul style="list-style-type: none">• Operations control• Facilities Management• Event Management• Incident Management• Access Management• Problem Management	--
Eu.Sec.596	Info	<ul style="list-style-type: none">• Service Strategy (for security related aspects)<ul style="list-style-type: none">• Demand Management: Threat landscape• Deliverables: Risk-Management/-assessment, Strategies, Policies, Objectives, Requirements	--
Eu.Sec.597	Info	Some of the above-mentioned elements shall be exclusively dedicated to managing and operate the security infrastructure. This counts for: <ul style="list-style-type: none">• Information Security Management: for Security infrastructure• Supplier Management: for Security infrastructure• IT Service Continuity Management: for Security infrastructure	--
Eu.Sec.598	Info	The element "Identity management" is not from ITIL and arises out of the Access Management which relies on identifiable assets and the importance of the authentication of safety relevant components.	--

Figure 1: From object 649 on page 9.

