



**EULYNX Initiative**

## **EULYNX Security Specification**

Document number: Eu.Doc.114  
Version: 1.1 (0.A)

Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
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
<b>2</b>	<b>Security Measures</b>	<b>3</b>
2.1	Introduction	3
2.2	Identification and Authentication (IAC)	3
2.2.1	M00043: Identity and Access Management	3
2.2.1.1	General	3
2.2.1.2	Concept of using an IAM	5
2.2.1.3	Identity Management	5
2.2.1.4	Procedural requirements	6
2.2.1.4.1	Usage	6
2.2.1.4.2	Check	6
2.2.1.4.3	Change	7
2.2.1.5	Access Management	7
2.2.1.6	Requirements for Network Access Control	7
2.2.1.6.1	General	7
2.2.1.6.2	Wireline	7
2.2.1.6.3	Wireless	8
2.2.1.6.4	Technical Process	8
2.2.2	M00067: Public Key Infrastructure	8
2.2.2.1	General	8
2.2.2.2	Introduction	8
2.2.2.3	Purpose	8
2.2.2.4	Architecture of the PKI	10
2.2.2.5	General requirements	10
2.2.2.6	Request a certificate during (re)commissioning	11
2.2.2.7	Renew a certificate	11
2.2.2.8	Revoke a certificate	11
2.2.2.9	Validate a certificate	12
2.2.2.10	Certificate	12

2.2.2.11	Lifespan of certificates	12
2.2.2.12	Trust model	12
2.2.2.13	Time synchronisation	13
2.2.3	M00044: Unique usage of certificates/identities	13
2.2.3.1	General	13
2.2.4	M00056: Segregation of duties and privilege separation	13
2.2.4.1	General	13
2.2.5	M00066: Authorisation of SCI machine-to-machine communication	14
2.2.5.1	General	14
2.3	Use Control (UC)	15
2.3.1	M00006: Alert personnel in case of detected unfavourable climatic conditions	15
2.3.1.1	General	15
2.3.2	M00037: Security checks for personnel	15
2.3.2.1	General	15
2.3.3	M00042: Dual control principle for administration	16
2.3.3.1	General	16
2.3.4	M00057: Analysis of administrator behaviour	16
2.3.4.1	General	17
2.4	System Integrity (SI)	17
2.4.1	M00021: Protect integrity of devices	17
2.4.1.1	General	17
2.4.1.2	EfeS, SCS, ILS-Adapter	18
2.4.2	M00023: Cryptographic integrity protection	18
2.4.2.1	General	18
2.4.2.2	Network-specific Measure / Data (information) in transit	19
2.4.2.3	Data (information) at rest	19
2.4.3	M00028: Protection of software and configuration updates	19
2.4.3.1	General	19
2.4.4	M00052: Separation of safety and security	20
2.4.4.1	General	20
2.5	Data Confidentiality (DC)	20
2.5.1	M00019: Limitation of security-relevant emissions	20
2.5.1.1	General	20
2.5.2	M00020: Protection of private keys	21
2.5.2.1	General	21
2.5.3	M00024: Data confidentiality	21
2.5.3.1	General	21
2.5.3.2	Data in transit	22
2.5.3.3	Data at rest	23
2.5.3.4	Data in process	23
2.6	Restricted Data Flow (RDF)	23
2.6.1	M00051: Network segmentation	23

2.6.1.1	General	23
2.6.2	M00053: Firewall and intrusion detection	24
2.6.2.1	General	24
2.6.2.2	EfeS and ILS-Adapter	24
2.6.2.3	EIL, MDM and SSP	24
2.7	Timely Response to Events (TRE)	25
2.7.1	M00022: Central logging and event management	25
2.7.1.1	General	25
2.7.1.1.1	MDM	26
2.7.1.1.2	SCS	26
2.7.1.2	General logging requirements	26
2.7.2	M00040: Network monitoring	26
2.7.2.1	General	26
2.7.3	M00059: Local log storage and juridical recording	27
2.7.3.1	General	27
2.8	Resource Availability (RA)	27
2.8.1	M00007: Highly available and protected air conditioning	27
2.8.1.1	General	27
2.8.2	M00012: Network resilience against single point of failure	27
2.8.2.1	General	28
2.8.2.2	SCS	28
2.8.3	M00013: Emergency Power Supply	28
2.8.3.1	General	28
2.8.3.2	EIL	29
2.8.4	M00030: Backup of device data	29
2.8.4.1	General	29
2.8.5	M00033: Spare parts	30
2.8.5.1	General	30
2.8.6	M00039: System hardening	30
2.8.6.1	General	30
2.8.7	M00060: Protection against Denial of Service (DoS)	31
2.8.7.1	General	31
2.8.7.2	SCS	31
2.8.7.3	MDM, SSP, EIL	31
2.8.8	M00064: Limit resources of security functions	31
2.8.8.1	General	31
2.9	Organisational Security and Processes (OSP)	32
2.9.1	M00003: Integrate security into processes	32
2.9.1.1	General	32
2.9.1.2	EIL, MDM, SSP, EfeS, and ILS-Adapter	32
2.9.1.3	Patch-Process	32
2.9.1.4	Vulnerability Management	37

2.9.1.5	First operation and re-commissioning	44
2.9.1.6	Decommissioning	44
2.9.1.7	Documentation	45
2.9.1.8	Monitoring	46
2.9.2	M00014: Supply chain security	46
2.9.2.1	General	46
2.9.2.2	Supplier Management	46
2.9.2.3	Production	47
2.9.2.4	Transport	47
2.9.2.5	Commissioning process	47
2.9.3	M00016: Procurement strategy	47
2.9.3.1	General	47
2.9.4	M00017: Management of service providers	48
2.9.4.1	General	48
2.9.5	M00034: Detecting security vulnerabilities	48
2.9.5.1	General	48
2.9.5.2	Vulnerability scanning	49
2.9.5.3	Penetration-testing	49
2.9.6	M00035: Integration of security measures and components in railway operation procedures	49
2.9.6.1	General	49
2.9.7	M00038: Security Awareness trainings for personnel	50
2.9.7.1	General	50
2.9.8	M00041: Dual control principle in software development	50
2.9.8.1	General	50
2.9.9	M00048: Testing procedures	51
2.9.9.1	General	51
2.9.9.2	Functionality Testing	51
2.9.9.3	Security Related Component Testing	51
2.9.9.4	Security Integration Testing	52
2.9.9.5	Security Testing Procedures	52
2.9.9.5.1	Analyse specifications and pre-existing tests	53
2.9.9.5.2	Functional test	53
2.9.9.5.3	Pre-integration test	54
2.9.9.5.4	System integration test	54
2.9.9.5.5	Field test	54
2.9.9.5.6	Operational tests	54
2.9.10	M00049: Human resources planning and training	54
2.9.10.1	General	54
2.9.11	M00055: Privacy related information	54
2.9.11.1	General	54
2.10	Physical Protection (PP)	55
2.10.1	M00002: Physical protection	55

2.10.1.1	General	55
2.10.2	M00005: Rules for locations with major importance	55
2.10.2.1	General	55
2.10.3	M00010: Rules for locations with minor importance	56
2.10.3.1	General	56
2.10.3.2	SCS	56
2.10.4	M00008: Design components according to EN50125-3	56
2.10.4.1	General	56
2.10.5	M00009: Design housing according to EN50600	57
2.10.5.1	General	57
2.10.6	M00011: Design physical intrusion protection for shelter or cubicle	58
2.10.6.1	General	58
2.10.7	M00018: Electromagnetic Compatibility (EMC)	58
2.10.7.1	General	58
2.10.8	M00032: Anti-Theft	59
2.10.8.1	General	59
2.10.9	M00063: Physical protection of unprotected communication	59
2.10.9.1	General	59

ID	Type	Requirement	Valid for
Eu.SecSpec.8	Head	<b>1 Introduction</b>	
Eu.SecSpec.9	Head	<b>1.1 Release information</b>	
Eu.SecSpec.10	Info	[Eu.Doc.114] EULYNX Security Specification CENELEC Phase: 4 Version: 1.1 (0.A) Approval date: 15.06.2023	--
Eu.SecSpec.21	Info	<b>Version history</b>	--
Eu.SecSpec.22	Info	version number: 0.1 (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: initial version in Doors	--
Eu.SecSpec.2731	Info	version number: 1.0 (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.SecSpec.2813	Info	version number: 1.1 (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.SecSpec.23	Head	<b>1.2 Impressum</b>	
Eu.SecSpec.24	Info	Publisher: <b>EULYNX Initiative</b>  A full list of the <b>EULYNX Partners</b> can be found on <a href="http://www.eulynx.eu/index.php/members">www.eulynx.eu/index.php/members</a>	--
Eu.SecSpec.26	Info	Responsible for this document: EULYNX Project Management Office <a href="http://www.eulynx.eu">www.eulynx.eu</a>	--
Eu.SecSpec.28	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.11].	--
Eu.SecSpec.29	Head	<b>1.3 Purpose</b>	
Eu.SecSpec.31	Info	The purpose of this document is to define the security requirements on specification 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.SecSpec.32	Info	This document covers the security requirements specification for EULYNX following the principles of the EULYNX Security Concept [Eu.Doc.15].	--
Eu.SecSpec.34	Info	The concept for security is documented in the EULYNX Security Concept [Eu.Doc.15].	--
Eu.SecSpec.36	Info	Inputs for the document are the systems operational environment, applicable security standards as well as purpose and scope of the system.	--
Eu.SecSpec.38	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.	--
Eu.SecSpec.39	Req	All requirements are based on the EULYNX risk assessment. If the IM is not following these recommendations, the IM must ensure that his security level is maintained.	IM

ID	Type	Requirement	Valid for
Eu.SecSpec.2809	Info	This document is intended for the following users: <ul style="list-style-type: none"> <li>• safety authorities</li> <li>• infrastructure managers</li> <li>• safety assessors</li> <li>• signalling system suppliers</li> <li>• validators</li> <li>• security assessors</li> </ul>	--
Eu.SecSpec.2810	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.SecSpec.2808	Info	The following statements should be considered before applying the specification: <ul style="list-style-type: none"> <li>• The security documents of the following enumeration shall be referred and used only as a complete set. <ul style="list-style-type: none"> <li>o Eu.Doc.15</li> <li>o Eu.Doc.114</li> <li>o Eu.Doc.115</li> <li>o Eu.Doc.116</li> <li>o Eu.Doc.117</li> <li>o Eu.Doc.121</li> </ul> </li> <li>• Development of the specification is based on IEC 62443 process, together with TS 50701 railway specification application suggestions.</li> <li>• 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.</li> <li>• 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).</li> <li>• 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.</li> </ul>	--
Eu.SecSpec.43	Head	<b>1.4 Applicable standards and regulations</b>	
Eu.SecSpec.75	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.SecSpec.76	Info	Standards referred by these railway standards are not referred.	--
Eu.SecSpec.45	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].	--
Eu.SecSpec.78	Info	This document is written based on the following standards: <ol style="list-style-type: none"> <li>1) TS 50701 [EU.Ref.191]</li> <li>2) IEC 62443 [EU.Ref.35] <ul style="list-style-type: none"> <li>IEC 62443-2-1</li> <li>IEC 62443-3-2</li> <li>IEC 62443-3-3</li> <li>IEC 62443-4-1</li> <li>IEC 62443-4-2</li> </ul> </li> <li>3) EN 50159 [EU.Ref.52]</li> <li>4) EN 50126 [EU.Ref.49]</li> <li>5) EN 50128 [EU.Ref.50]</li> <li>6) EN 50129 [EU.Ref.51]</li> <li>7) ISO 27001 [EU.Ref.189]</li> </ol> <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.SecSpec.90	Info	If one of the referenced standards shall be applied in addition to requirements in this document, it is stated explicitly.	--
Eu.SecSpec.47	Head	<b>1.5 Applicable documents</b>	
Eu.SecSpec.49	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.SecSpec.52	Head	<b>1.6 Terms and abbreviations</b>	
Eu.SecSpec.54	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].	--
Eu.SecSpec.57	Head	<b>1.7 Variability management</b>	
Eu.SecSpec.59	Info	This document is valid for the complete EULYNX System. Variability management is not used in this document.	--
Eu.SecSpec.60	Head	<b>1.8 Definition of object types</b>	
Eu.SecSpec.62	Info	The following definition for object types is applied in this document:	--
Eu.SecSpec.64	Info	• "Req" - This denotes a mandatory requirement.	--
Eu.SecSpec.66	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.	--
Eu.SecSpec.68	Info	• "Head" - This denotes chapter headings.	--
Eu.SecSpec.70	Head	<b>2 Security Measures</b>	
Eu.SecSpec.71	Head	<b>2.1 Introduction</b>	
Eu.SecSpec.73	Info	All requirements and recommendations are made with the knowledge as of November 2021. It is expected that these requirements will change. These changes must be managed by the life-cycle management of the IM in contact with the supplier. EULYNX will update following their release or baseline planning.	--
Eu.SecSpec.92	Info	The following measures are based on a threat-based risk assessment for the EULYNX architecture. Details can be found in the EULYNX Security Concept [Eu.Doc.15].	--
Eu.SecSpec.94	Info	All assumptions and the scope of the measures are documented in the EULYNX Security Threat and Risk Analysis [EU.Doc.116], and the EULYNX Security Concept [Eu.Doc.15].	--
Eu.SecSpec.95	Info	The following major assumptions are:	--
Eu.SecSpec.96	Info	• Security level 3 (IEC 62443), meaning a highly capable criminal organisation but not nation state attackers	--
Eu.SecSpec.97	Info	• Organisational maturity tier 4 (NIST) or ML 4 (IEC 62443), meaning repeatable processes and timely, continuous improvement	--
Eu.SecSpec.98	Info	• Only attacks targeting safety and/or availability of railway operation are considered.	--
Eu.SecSpec.100	Info	For SCI-XX the protection requirements analysis result was, that no confidentiality requirements have to be applied. Thus only integrity and availability are relevant. Note: There are confidentiality requirements e.g., for private keys, SMI and SDI network traffic. Note: The risk assessment and corresponding results might have to be changed due to new security research findings and higher estimations of the attacker's capability. The risk of reconnaissance on unencrypted connections based on the encryption requirements of M00024 is considered low in the EULYNX Security Threat and Risk Analysis [EU.Doc.116]. The reconnaissance phase or information gathering for attack timing/coordination could analyse e.g., the SCI-xx command network traffic to attack safety or availability of the railway operation.	--
Eu.SecSpec.101	Req	If the IM's protection requirements analysis does require confidentiality for SCI-XX, the IM shall apply Security Measure M00024.	IM
Eu.SecSpec.103	Info	The IM or supplier is free to add additional measures and to extend functionality as long as the set security level is not negatively affected.	--
Eu.SecSpec.105	Req	If additional functionality or measures are defined by the IM, the IM shall maintain interoperability.	IM
Eu.SecSpec.107	Req	If additional functionality or measures are defined by the supplier, the supplier shall maintain interoperability.	All
Eu.SecSpec.108	Head	<b>2.2 Identification and Authentication (IAC)</b>	
Eu.SecSpec.109	Head	<b>2.2.1 M00043: Identity and Access Management</b>	
Eu.SecSpec.2742	Head	<b>2.2.1.1 General</b>	
Eu.SecSpec.111	Info	Measure ID: M00043	--

ID	Type	Requirement	Valid for
Eu.SecSpec.112	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• SCS</li> </ul>	--
Eu.SecSpec.118	Info	Threats: <ul style="list-style-type: none"> <li>• T 023 Unauthorised Access to IT Systems</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 032 Abuse of Authorisations</li> <li>• T 035 Coercion, Extortion or Corruption</li> <li>• T 036 Identity Theft</li> <li>• T 041 Sabotage</li> <li>• T 042 Social Engineering</li> <li>• T 043 Replaying Messages</li> <li>• T 044 Unauthorised Entry to Premises</li> <li>• T 045 Data Loss</li> </ul>	--
Eu.SecSpec.129	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 1.1, SR 1.1 RE1, SR 1.1 RE 2</li> <li>• SR 1.2, SR 1.2 RE 1</li> <li>• SR 1.3, SR 1.3 RE 1</li> <li>• SR 1.4</li> <li>• SR 1.5</li> <li>• SR 1.7</li> <li>• SR 1.10</li> <li>• SR 1.11</li> <li>• SR 1.13</li> <li>• SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2</li> <li>• SR 2.5</li> <li>• SR 2.6</li> <li>• SR 2.11 RE 1</li> </ul>	--
Eu.SecSpec.2814	Req	If the component provides an human-to-machine interface, the component shall check user authentications using a connection to the SSP-IAM service.	All
Eu.SecSpec.3141	Req	If the component provides an human-to-machine interface, the component shall check user authorisation using a connection to the SSP-IAM service.	All
Eu.SecSpec.147	Req	The IAM shall provide the components with the ability to authenticate all human users.	All
Eu.SecSpec.148	Req	The IAM shall provide the function of the segregation of duty principle.	All
Eu.SecSpec.2816	Req	The rights management of the IAM shall be established using the segregation of duty principle.	All
Eu.SecSpec.149	Req	The identifier management of the IAM shall be established according to IEC 62443 SR 1.4.	All
Eu.SecSpec.150	Req	The IAM shall synchronize personnel data with the personnel database.	All
Eu.SecSpec.2817	Req	The IAM shall synchronize personnel data with the personnel database once a day.	All
Eu.SecSpec.2818	Req	The IAM shall be synchronized with the personnel database fully automated.	All
Eu.SecSpec.151	Req	The IAM shall provide log data using SSI-XX-SLOG to the SSP-SLOG service.	All
Eu.SecSpec.152	Req	The IAM shall support strong passwords according to national regulation.	All
Eu.SecSpec.2819	Req	The IAM password rules shall be configurable.	All
Eu.SecSpec.3129	Req	If passwords are used, the IM shall provide the applicable password rules.	IM
Eu.SecSpec.153	Req	The IAM shall use obscured authentication process feedback according to IEC 62443 SR 1.10.	All
Eu.SecSpec.154	Req	The component shall limit the number of invalid access attempts according to IEC 62443 SR 1.11.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2820	Req	The component's number of invalid access attempts shall be configurable.	All
Eu.SecSpec.155	Req	The component shall lock sessions according to IEC 62443 SR 2.5 and SR 2.6	All
Eu.SecSpec.2821	Req	The component shall provide the ability to terminate remote sessions automatically after a configurable in-active time.	All
Eu.SecSpec.157	Req	The component shall provide the ability to synchronize component time using SDI time synchronization interface.	All
Eu.SecSpec.169	Head	<b>2.2.1.2 Concept of using an IAM</b>	
Eu.SecSpec.171	Info	Using Identity and Access Management services, short IAM, enables centralized management and timely updates to grant or revoke access to a device, service, or functionality.	--
Eu.SecSpec.172	Info	IAM is always based on identities and their digital representation. The public key infrastructure (PKI) is offering this digital representation with certificates, together with the required technical services to issue, renew, revoke, and validate them.	--
Eu.SecSpec.173	Info	IAM is closely related to asset management as well as human resource administration. Procedural and technical interfaces must be implemented to meet timeliness.	--
Eu.SecSpec.174	Info	All technical functionality required to manage access real-time or near real time must be implemented to a certain extend in the components of the EULYNX subsystems. To avoid unwanted complexity in the IAM, this functionality in the subsystems is relevant for interoperability and therefore subject to harmonisation.	--
Eu.SecSpec.175	Head	<b>2.2.1.3 Identity Management</b>	
Eu.SecSpec.178	Info	For EULYNX these will include amongst others instances of the following types:	--
Eu.SecSpec.179	Info	• People	--
Eu.SecSpec.180	Info	• Devices	--
Eu.SecSpec.181	Info	• Systems	--
Eu.SecSpec.182	Info	• Services	--
Eu.SecSpec.183	Info	• Processes	--
Eu.SecSpec.184	Info	• Interface Endpoints	--
Eu.SecSpec.189	Info	• Functions	--
Eu.SecSpec.190	Info	• Commands	--
Eu.SecSpec.193	Info	All EULYNX devices and systems operated by an IM, are part of one, single domain. Other domains might be from other IMs or NON-EULYNX devices and systems.	--
Eu.SecSpec.194	Info	Federation of different domains must be setup up between the domain holders. Especially federation for IAM for people should be implemented. How to implement is largely depending on the technical systems available at the IM.	--
Eu.SecSpec.195	Req	The IAM shall ensure that the identity of each instance is assigned to a certificate issued by the PKI.	All
Eu.SecSpec.197	Req	The IM shall define procedures to securely identify an instance and assigning the digital identity.	IM
Eu.SecSpec.2822	Req	The component shall provide the IM with the ability to check its identity physically during the commissioning process.	All
Eu.SecSpec.205	Req	The IAM shall provide the capability of multi-factor authentication.	All
Eu.SecSpec.3142	Req	If the component provides an human-to-machine interface, the component shall support multi-factor authentication to check the authentication of human users.	All
Eu.SecSpec.209	Req	The IAM shall support interfaces to an asset management.	All
Eu.SecSpec.2823	Req	The IAM shall be connected to an asset management.	All
Eu.SecSpec.211	Req	The IAM shall support interfaces to a corporate directory for user accounts synchronisation	All
Eu.SecSpec.2824	Req	The IAM shall be connected to a corporate directory for user accounts synchronisation.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.213	Req	The IAM shall provide a unique identity for components.	All
Eu.SecSpec.216	Req	During the life-time of a component the IAM shall provide the capability to keep the identity for each components throughout their lifetime.	All
Eu.SecSpec.218	Req	The IAM shall provide the capability of User to Role mapping.	All
Eu.SecSpec.2825	Req	The IAM shall provide the capability of Role to Permission mapping.	All
Eu.SecSpec.219	Req	The IAM shall provide the capability to group identities.	All
Eu.SecSpec.2826	Req	The IAM shall provide the capability that identities can belong to multiple groups.	All
Eu.SecSpec.221	Req	The IAM shall provide the capability of hierarchical identity structures.	All
Eu.SecSpec.2827	Req	The hierarchical identity structure of the IAM shall represent the logical structure of the system.	All
Eu.SecSpec.2828	Req	The IAM shall provide the capability to add attributes to identities.	All
Eu.SecSpec.227	Req	The IAM shall provide the capability to manage the current state of an identity.	All
Eu.SecSpec.2829	Info	The state of an identity may be currently operational, last operational status of the overall system, planning state, etc.	--
Eu.SecSpec.235	Info	Depending on application and the processes defined by the IM, the instance has its identity right from the start of life or has it starting with putting it in operation, e.g. are spare EfeS already known in the NAC or not.	--
Eu.SecSpec.236	Info	Example: The proof of identity may be done with a self-signed certificate combined with additional processes. Alternatively, the device has a manufacturer certificate, this could be used to distribute the "working certificate/identity" to the entity. The IM decides which variant is to be used for what application.	--
Eu.SecSpec.237	Info	Note: Using a self-signed certificate for proof of identity could be with regard to the process steps similar to setting up WiFi connection using WPA enterprise (WPA 3).	--
Eu.SecSpec.239	Req	The IM shall define certificate issuing use cases for the PKI.	IM
Eu.SecSpec.241	Req	Before commissioning the component shall get a manufacturer certificate.	All
Eu.SecSpec.2830	Req	The IM shall define the commissioning process for each component.	IM
Eu.SecSpec.2831	Info	The manufacturer certificate could play a role in the (first-time) identification/authentication process, depending on the level of trust. The requirements for the certificates with TLS apply.	--
Eu.SecSpec.349	Head	<b>2.2.1.4 Procedural requirements</b>	
Eu.SecSpec.361	Head	<b>2.2.1.4.1 Usage</b>	
Eu.SecSpec.363	Req	At every startup, the component shall perform the authorisation procedure.	All
Eu.SecSpec.364	Head	<b>2.2.1.4.2 Check</b>	
Eu.SecSpec.366	Req	Each component shall enforce authorisation by checking the validity of the granted access at least every 12 hours.	All
Eu.SecSpec.2841	Req	Each component shall provide the capability to configure the validity time interval.	All
Eu.SecSpec.368	Req	The IM shall define the interval of the validity check on component level.	IM
Eu.SecSpec.2842	Info	The parameter of checking the access interval shall be in line with the security policies of the IM and the practical feasibility in daily operation.	--
Eu.SecSpec.370	Req	The IM shall regularly check the accounts for compliance to the security policy.	IM
Eu.SecSpec.372	Req	The IM shall regularly check the hierarchical structure for compliance to the security policy.	IM
Eu.SecSpec.374	Info	The security policies could include:	--
Eu.SecSpec.375	Info	<ul style="list-style-type: none"><li>Rules for use case: join, leave and move</li></ul>	--
Eu.SecSpec.376	Info	<ul style="list-style-type: none"><li>Rules for suitable privilege levels</li></ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.378	Req	The IM shall define identity hierarchical structure and the according roles based on use cases.	IM
Eu.SecSpec.379	Head	<b>2.2.1.4.3 Change</b>	
Eu.SecSpec.381	Req	When roles, responsibilities and groups are changed, the IM shall check the rights of the assigned users.	IM
Eu.SecSpec.2843	Req	The IAM shall provide the capability to enforce approval for changes of role permissions or user to role assignment.	All
Eu.SecSpec.383	Info	Changes become effective at the next regular authorization enforcement.	--
Eu.SecSpec.242	Head	<b>2.2.1.5 Access Management</b>	
Eu.SecSpec.244	Req	The component shall be connected to an IAM.	All
Eu.SecSpec.2832	Req	The IAM shall be managed centrally.	All
Eu.SecSpec.2833	Req	The component shall only allow access based on the rights managed in the IAM.	All
Eu.SecSpec.248	Req	The IM shall define processes to manage access.	IM
Eu.SecSpec.250	Req	The IAM shall grant access to components using roles.	All
Eu.SecSpec.252	Req	The roles used by the IAM shall be defined based on a set of permissions.	All
Eu.SecSpec.254	Req	The IM shall assign roles to components in the IAM.	IM
Eu.SecSpec.2834	Req	The IM shall assign users to roles in the IAM.	IM
Eu.SecSpec.2835	Req	The IM shall assign permissions to roles in the IAM.	IM
Eu.SecSpec.310	Req	The IAM service shall use the time provided by time service.	All
Eu.SecSpec.317	Req	The component shall enforce the authorisations of users requesting access.	All
Eu.SecSpec.775	Head	<b>2.2.1.6 Requirements for Network Access Control</b>	
Eu.SecSpec.776	Info	These requirements for network access control apply only between EULYNX field element Subsystem or interlocking to the first transport network element.	--
Eu.SecSpec.777	Req	Only if variant B or C is chosen, the component shall fulfil the NAC requirements.	All
Eu.SecSpec.779	Req	Appropriate processes shall be implemented to react on alerts from network access control.	IM
Eu.SecSpec.780	Head	<b>2.2.1.6.1 General</b>	
Eu.SecSpec.782	Info	Access control should be managed in a way to grant or remove the permission to access the network and should support timely reaction in case of Denial of Service type incidents without generating unacceptable side effects (availability, mission: run trains).	--
Eu.SecSpec.783	Info	The connecting device should implement the functionality for a client/supplicant.	--
Eu.SecSpec.784	Info	The endpoint of the transport network should implement the functionality of an authenticator.	--
Eu.SecSpec.785	Info	The management system should implement the functionality of an authentication server.	--
Eu.SecSpec.786	Info	As the NAC functionality is between the authentication server and the authenticator, the operator of the transport network is free choosing which methods to be used (e.g. RADIUS, LDAP, TACACS, ...).	--
Eu.SecSpec.787	Info	NAC affects availability; hence this aspect must be considered. (e.g. time to grant a port, port-flapping issues, certificate changes, scalability (e.g. every EfeS has >=1 ports),...).	--
Eu.SecSpec.2870	Req	The network access control shall enforce the deny-by-default principle.	All
Eu.SecSpec.788	Head	<b>2.2.1.6.2 Wireline</b>	
Eu.SecSpec.789	Req	The component shall authenticate to the network using NAC according to EAP-TLS 802.1x-2020.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2871	Req	The SCS shall implement NAC using EAP-TLS 802.1x-2020.	All
Eu.SecSpec.799	Head	<b>2.2.1.6.3 Wireless</b>	
Eu.SecSpec.800	Info	Network access control mechanisms of wireless networks should be implemented if wireless connection are used.	--
Eu.SecSpec.803	Info	Cell based mobile networks, e.g. 3G, 4G, 5G, FRMCS, implement access control enforced by using SIM or eSIM. Based on device authentication there are closed user groups similar to NAC.	--
Eu.SecSpec.804	Info	Cell based mobile network NAC functionality may be required as an application condition and will be implemented by the mobile network operator.	--
Eu.SecSpec.805	Head	<b>2.2.1.6.4 Technical Process</b>	
Eu.SecSpec.815	Req	The authentication server shall provide the capability to allow policy handling to enable connectivity association.	All
Eu.SecSpec.816	Req	The component shall support periodic re-authentication during an active session using NAC according to EAP-TLS 802.1x-2020.	All
Eu.SecSpec.817	Req	The component shall support separate re-authentication per network interface using NAC according to EAP-TLS 802.1x-2020.	All
Eu.SecSpec.2872	Info	Separate re-authentication may ensure that at least one connection stays active - also if re-authentication fails for availability reasons.	--
Eu.SecSpec.396	Head	<b>2.2.2 M00067: Public Key Infrastructure</b>	
Eu.SecSpec.3140	Head	<b>2.2.2.1 General</b>	
Eu.SecSpec.3136	Info	Measure ID: M00067	--
Eu.SecSpec.3137	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• EfeS</li><li>• MDM</li><li>• SSP</li><li>• SCS</li><li>• ILS-Adapter</li><li>• TCS</li><li>• RBC</li></ul>	--
Eu.SecSpec.3138	Info	Threats: <ul style="list-style-type: none"><li>• T 030 Unauthorised Use or Administration of Devices and Systems</li><li>• T 031 Incorrect Use or Administration of Devices and Systems</li><li>• T 032 Abuse of Authorisations</li><li>• T 035 Coercion, Extortion or Corruption</li><li>• T 036 Identity Theft</li><li>• T 041 Sabotage</li><li>• T 042 Social Engineering</li><li>• T 044 Unauthorised Entry to Premises</li></ul>	--
Eu.SecSpec.3139	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SR 1.8</li><li>• SR 1.9</li></ul>	--
Eu.SecSpec.397	Head	<b>2.2.2.2 Introduction</b>	
Eu.SecSpec.399	Info	The issued certificates confirm the authenticity of further certification authorities, digital signatures or of encryption keys. The certificates are issued to users or devices. Certificates support authentication of communication endpoint, this is a major capability to secure interfaces like SCI, SMI, SDI and SSI.	--
Eu.SecSpec.401	Info	This chapter refers the word "key" for key information which needs to be kept secret, e.g., private keys in a public key environment or symmetric keys. Key information which requires not to be secret are referred as "public keys".	--
Eu.SecSpec.402	Head	<b>2.2.2.3 Purpose</b>	
Eu.SecSpec.404	Info	The PKI provides certificates corresponding to digital identities for each entity.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.406	Info	Subject is identical to "end entity (EE)": entity to whom the certificate is issued (RFC4210: 3.1.1.1). Subject not to be used in order not to confuse with "subject field " in the certificate.	--
Eu.SecSpec.407	Info	Use cases:	--
Eu.SecSpec.408	Info	<ul style="list-style-type: none"> <li>• end user use cases, e.g. authentication between two communication participants</li> </ul>	--
Eu.SecSpec.409	Info	<ul style="list-style-type: none"> <li>• sign data</li> </ul>	--
Eu.SecSpec.410	Info	<ul style="list-style-type: none"> <li>• sign data for non-repudiation</li> </ul>	--
Eu.SecSpec.411	Info	<ul style="list-style-type: none"> <li>• sign software/firmware</li> </ul>	--
Eu.SecSpec.412	Info	<ul style="list-style-type: none"> <li>• secure boot</li> </ul>	--
Eu.SecSpec.413	Info	<ul style="list-style-type: none"> <li>• integrity-protected or encrypt communication, e.g.:</li> </ul>	--
Eu.SecSpec.414	Info	<ul style="list-style-type: none"> <li>• TLS</li> </ul>	--
Eu.SecSpec.415	Info	<ul style="list-style-type: none"> <li>• OPC UA Binary: Secure Conversation</li> </ul>	--
Eu.SecSpec.416	Info	<ul style="list-style-type: none"> <li>• IPsec, e.g. to be used in Crypto Box type VPNs</li> </ul>	--
Eu.SecSpec.417	Info	<ul style="list-style-type: none"> <li>• authentication of an entity (person, device, service, ...)</li> </ul>	--
Eu.SecSpec.418	Info	<ul style="list-style-type: none"> <li>• authentication for SSH</li> </ul>	--
Eu.SecSpec.419	Info	<ul style="list-style-type: none"> <li>• authentication for network access control (NAC)</li> </ul>	--
Eu.SecSpec.421	Info	<ul style="list-style-type: none"> <li>• Revoking certificates due to security incident or (potentially) compromised systems.</li> </ul>	--
Eu.SecSpec.422	Info	<ul style="list-style-type: none"> <li>• Revoking during decommissioning.</li> </ul>	--
Eu.SecSpec.423	Info	<ul style="list-style-type: none"> <li>• First-time certificate on the device (either from supplier or using an automated certificate request)</li> </ul>	--
Eu.SecSpec.424	Info	<ul style="list-style-type: none"> <li>• Software updates / retrofit programs.</li> </ul>	--
Eu.SecSpec.425	Info	<ul style="list-style-type: none"> <li>• Bulk changes for request, issuing and provisioning of certificates (e.g. "root CA" has to be changed)</li> </ul>	--
Eu.SecSpec.426	Info	<ul style="list-style-type: none"> <li>• certificate handling with supplier:</li> </ul>	--
Eu.SecSpec.427	Info	<ul style="list-style-type: none"> <li>• purchase, logistic: new devices delivered.</li> </ul>	--
Eu.SecSpec.428	Info	<ul style="list-style-type: none"> <li>• 3<sup>rd</sup> level support: connecting services during maintenance.</li> </ul>	--
Eu.SecSpec.429	Info	<ul style="list-style-type: none"> <li>• cross-acceptance with CA from suppliers or operators, national or international</li> </ul>	--
Eu.SecSpec.434	Req	The PKI shall provide the capability to request a certificate.	All
Eu.SecSpec.435	Req	The PKI shall provide the capability to renew a certificate.	All
Eu.SecSpec.436	Req	The PKI shall provide the capability to revoke a certificate.	All
Eu.SecSpec.437	Req	The PKI shall provide the capability to validate a certificate.	All
Eu.SecSpec.2844	Req	The component shall support the PKI capability to request a certificate.	All
Eu.SecSpec.2845	Req	The component shall support the PKI capability to renew a certificate.	All
Eu.SecSpec.2846	Req	The component shall support the PKI capability to revoke a certificate.	All
Eu.SecSpec.2847	Req	The component shall support the PKI capability to validate a certificate.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.438	Head	<b>2.2.2.4 Architecture of the PKI</b>	
Eu.SecSpec.440	Info	The PKI architecture has the following elements:	--
Eu.SecSpec.441	Info	• End entity / subject	--
Eu.SecSpec.442	Info	• Personal Security Environment (PSE) (RFC4210: 3.1.1.1)	--
Eu.SecSpec.443	Info	• Registration Authority (RA)	--
Eu.SecSpec.444	Info	• Certificate Authority (CA) structure:	--
Eu.SecSpec.445	Info	• root CA (RFC4210: 3.1.1.2)	--
Eu.SecSpec.446	Info	• subordinate CA (RFC4210: 3.1.1.2)	--
Eu.SecSpec.447	Info	• intermediate CA	--
Eu.SecSpec.448	Info	• issuing CA	--
Eu.SecSpec.449	Info	• bridge CA	--
Eu.SecSpec.450	Head	<b>2.2.2.5 General requirements</b>	
Eu.SecSpec.456	Req	The EULYNX subsystem SCS shall use PKI services, if appropriate.	All
Eu.SecSpec.2848	Info	Examples are: network access control, implementing cat 1 or cat 2 networks, access control to SCS components.	--
Eu.SecSpec.458	Req	The IM shall define the quality expected for random number generation.	IM
Eu.SecSpec.2849	Info	Recommendations for random number generation can be found e.g. in BSI TR02102-1	--
Eu.SecSpec.2850	Req	The quality of the expected random number must be assessed and included into the risk management system.	IM
Eu.SecSpec.461	Req	The IM shall define availability requirements for the PKI according to the overall system concept.	IM
Eu.SecSpec.462	Req	The IM shall define availability requirements for the CA according to the overall system concept.	IM
Eu.SecSpec.463	Req	The IM shall define availability requirements for the Registration Authority according to the overall system concept .	IM
Eu.SecSpec.464	Req	The IM shall define availability requirements for the Validation Authority according to the overall system concept.	IM
Eu.SecSpec.465	Req	The IM shall define availability requirements for the CRL-Server according to the overall system concept.	IM
Eu.SecSpec.466	Req	If an OCSP-Responder is required, the IM shall define availability requirements for the OCSP-Responder according to the overall system concept.	IM
Eu.SecSpec.467	Req	The IM shall define availability requirements for the Time service according to the overall system concept.	IM
Eu.SecSpec.2851	Req	The PKI shall provide the availability required by the IM.	All
Eu.SecSpec.2852	Req	The CA shall provide the availability required by the IM.	All
Eu.SecSpec.2853	Req	The Registration Authority shall provide the availability required by the IM.	All
Eu.SecSpec.2854	Req	The Validation Authority shall provide the availability required by the IM.	All
Eu.SecSpec.2855	Req	The CRL-Server shall provide the availability required by the IM.	All
Eu.SecSpec.2856	Req	The OCSP responder shall provide the availability required by the IM.	All
Eu.SecSpec.2857	Req	The Time service shall provide the availability required by the IM.	All



ID	Type	Requirement	Valid for
Eu.SecSpec.470	Req	The component shall use SSI-XX-PKI for certificate management.	All
Eu.SecSpec.478	Req	The IM shall define the lifetime of certificate revocation lists based on risk assessments.	IM
Eu.SecSpec.479	Req	The IM shall define intervals for certificate validation based on risk assessments.	IM
Eu.SecSpec.2858	Req	The IAM shall be able to handle certificates from multiple certificate authorities.	All
Eu.SecSpec.2859	Req	The IAM shall be able to manage different roots of trust.	All
Eu.SecSpec.2860	Req	The PKI shall provide the capability to create alarms before certificates expire.	All
Eu.SecSpec.2861	Req	The PKI shall provide the capability to store the validation date of each issued certificate.	All
Eu.SecSpec.2862	Req	The PKI shall send an alarm before certificate expire to the Security Logging Service using SSI-XX-SLOG.	All
Eu.SecSpec.2863	Req	The PKI shall provide the capability to configure the time interval relative to certificate expiry before an alarm is created.	All
Eu.SecSpec.483	Head	<b>2.2.2.6 Request a certificate during (re)commissioning</b>	
Eu.SecSpec.492	Req	The network shall provide an isolated access to the PKI for Certificate Signing Requests (CSR) during the first time setup of the component.	All
Eu.SecSpec.233	Req	The component shall present an unambiguous proof of identity to the Registration Authority as part of requesting a certificate.	All
Eu.SecSpec.494	Req	The IM shall implement processes to ensure the authenticity of a CSR, which interact with first-time setup processes and maintenance processes (e.g. changing components).	IM
Eu.SecSpec.496	Info	For example, the maintenance worker triggers the CSR at the device and calling a RA agent by phone. The worker and the agent check if the CSR comply to the situation. the agent is then giving his document "ok" to the RA to accept the CSR.	--
Eu.SecSpec.497	Info	Or: The maintenance work has access to the RA to clear the CSR for that device. The access is protected by multi-factor authentication and is logged for juridical purposes.	--
Eu.SecSpec.498	Info	Or: Unique ID of a device/system is centrally or decentral supervised (e.g. distributed ledgers).	--
Eu.SecSpec.490	Req	The component shall request certificates according to RFC 2986.	All
Eu.SecSpec.2864	Req	The component shall transfer CSRs (Certificate Signing Requests - RFC 2986) to the Registration Authority using HTTP 1.1.	All
Eu.SecSpec.507	Req	The component shall protect private keys against theft and unauthorized use.	All
Eu.SecSpec.512	Head	<b>2.2.2.7 Renew a certificate</b>	
Eu.SecSpec.514	Info	The renewal process is based on a valid and for the renewal trusted certificate.	--
Eu.SecSpec.516	Req	The component shall initiate the renewal of its certificates automatically.	All
Eu.SecSpec.518	Req	The component shall renew certificates at least 10 days in advance to certificate expiry date.	All
Eu.SecSpec.520	Req	The component shall renew certificates on request via SMI.	All
Eu.SecSpec.2865	Info	The SMI trigger renewal is independent of expiry date of the certificate or its validity. The renewal command must be authorised and protected against replay attacks.	--
Eu.SecSpec.524	Info	The IM should periodically check if this process is working as intended.	--
Eu.SecSpec.525	Head	<b>2.2.2.8 Revoke a certificate</b>	
Eu.SecSpec.527	Info	A certificate is revoked at the CA. The CA provides the certificate revocation list or other means to the service to validate the certificate.	--
Eu.SecSpec.529	Req	The Certificate Authority shall add the CRL distribution point extension including the CRL distribution point address to every certificate issued.	All
Eu.SecSpec.2866	Req	The Certificate Authority shall add the Authority Information Access extension including the OCSP responder address to every certificate issued.	All
Eu.SecSpec.531	Req	The IM shall implement a process to revoke a certificate in a timely manner.	IM

ID	Type	Requirement	Valid for
Eu.SecSpec.533	Req	The IM shall implement a process to revoke a certificate, when a component is decommissioned.	IM
Eu.SecSpec.535	Info	It is recommended that a certificate is revoked if a device is off-monitoring for longer than 5 days. In addition, the IM should consider to re-assess hardware integrity of such devices.	--
Eu.SecSpec.540	Head	<b>2.2.2.9 Validate a certificate</b>	
Eu.SecSpec.545	Req	The component shall check if the certificate is signed by a trusted certificate authority	All
Eu.SecSpec.547	Req	The component shall check if the certificate is valid.	All
Eu.SecSpec.548	Req	The component shall check if the certificate is not revoked.	All
Eu.SecSpec.549	Info	Use case specific requirements may apply and should be checked accordingly.	--
Eu.SecSpec.555	Req	The component shall be able to manage multiple trusted certificate authorities.	All
Eu.SecSpec.560	Req	The component shall be able to check the certificate revocation status using CRLs.	All
Eu.SecSpec.561	Req	The component shall be able to check the certificate revocation status using OCSP following RFC 6960.	All
Eu.SecSpec.565	Req	The component shall provide the ability to be configured to use CRL only.	All
Eu.SecSpec.567	Req	The component shall provide the ability to be configured to use OCSP first, CRL second, if no OCSP connection is possible.	All
Eu.SecSpec.576	Req	The IM shall choose if the component shall only check the revocation status via CRLs.	IM
Eu.SecSpec.2867	Req	The IM shall choose if the component shall only check the revocation status via OCSP first and CRL as fall back.	IM
Eu.SecSpec.578	Req	The component shall update the local copy of a CRL before NextUpdate defined in the CRL.	All
Eu.SecSpec.610	Head	<b>2.2.2.10 Certificate</b>	
Eu.SecSpec.612	Req	The component shall be able to handle certificates as defined in the EULYNX Security Parameter Specification [Eu.Doc.115]	All
Eu.SecSpec.625	Req	The CA shall issue certificates which contain a unique commonName.	All
Eu.SecSpec.713	Head	<b>2.2.2.11 Lifespan of certificates</b>	
Eu.SecSpec.715	Req	The IM shall set the certificate lifespan and renewing according to his risk assessment.	IM
Eu.SecSpec.717	Info	The lifespan affects the time the certificate is still useful if a renewal procedure fails. As a result, renewal shall be done well before lifespan ends and alarming in case of failure and according action shall be implemented.	--
Eu.SecSpec.719	Req	The supplier shall limit the validity of supplier certificates used to authenticate communication to 3 years.	All
Eu.SecSpec.2868	Req	The IM shall ensure that the supplier certificate is replaced by an IM certificate within the commissioning process.	IM
Eu.SecSpec.2869	Req	The component shall not use supplier certificates if it is in operational mode.	All
Eu.SecSpec.720	Info	Certificate used for operational purpose should not exceed 6 months.	--
Eu.SecSpec.721	Info	Certificates used for test or assurance environments should not live longer than 1 year.	--
Eu.SecSpec.724	Head	<b>2.2.2.12 Trust model</b>	
Eu.SecSpec.726	Info	Trust models are described in RFC 4158.	--
Eu.SecSpec.730	Info	The question on "trust model" will not be decided in EULYNX but on a higher level, considering further aspects. (TSI, access to markets,...)	--
Eu.SecSpec.732	Info	Issues of national or international cross acceptance, e.g. border crossing, will not be decided in EULYNX but on a higher level, considering further aspects. (TSI, access to markets,...)	--
Eu.SecSpec.739	Info	There might be a need for legacy interoperability leading to an offline trust model. Offline trust models, commonly agreed audit rules and guidelines should be defined, assessed, and included into the IM's risk acceptance management. It is recommended to handle offline trust actions as "exceptions" in the ISMS.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.748	Head	<b>2.2.2.13 Time synchronisation</b>	
Eu.SecSpec.750	Info	Time synchronisation is not only required for security – but security requires it for certificate end-of-lifetime for TLS, NAC.	--
Eu.SecSpec.756	Info	It was discussed and assessed that the risk of NTP is very low. As a result, NTP with NTS ( <a href="https://tools.ietf.org/html/rfc8915">https://tools.ietf.org/html/rfc8915</a> , September 2020) is not mandatory.	--
Eu.SecSpec.820	Head	<b>2.2.3 M00044: Unique usage of certificates/identities</b>	
Eu.SecSpec.2743	Head	<b>2.2.3.1 General</b>	
Eu.SecSpec.822	Info	Measure ID: M00044	--
Eu.SecSpec.823	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.827	Info	Threats: <ul style="list-style-type: none"> <li>• T 023 Unauthorised Access to IT Systems</li> </ul>	--
Eu.SecSpec.829	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 1.1 RE1</li> <li>• SR 1.2, SR 1.2 RE 1</li> <li>• CR 1.9</li> </ul>	--
Eu.SecSpec.834	Req	The component shall provide the capability to handle separate certificates for each EULYNX interface.	All
Eu.SecSpec.2873	Req	The component shall provide the capability to handle separate certificates for NAC.	All
Eu.SecSpec.2874	Req	The component shall provide the capability to perform certificate signing requests separately for each EULYNX interface.	All
Eu.SecSpec.2875	Req	The component shall provide the capability to perform certificate signing requests separately for NAC.	All
Eu.SecSpec.2876	Req	The PKI shall provide separate certificates for each EULYNX interface.	All
Eu.SecSpec.2877	Req	The PKI shall provide separate certificates for NAC.	All
Eu.SecSpec.835	Head	<b>2.2.4 M00056: Segregation of duties and privilege separation</b>	
Eu.SecSpec.2744	Head	<b>2.2.4.1 General</b>	
Eu.SecSpec.837	Info	Measure ID: M00056	--
Eu.SecSpec.838	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.846	Info	Threats: <ul style="list-style-type: none"> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 031 Incorrect Use or Administration of Devices and Systems</li> <li>• T 032 Abuse of Authorisations</li> <li>• T 035 Coercion, Extortion or Corruption</li> <li>• T 036 Identity Theft</li> <li>• T 041 Sabotage</li> <li>• T 042 Social Engineering</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.855	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2</li> </ul>	--
Eu.SecSpec.858	Req	The IM shall define duties following the segregation of duty principle.	IM
Eu.SecSpec.860	Req	The IM shall define segregated duties which enforce separate approval and verification.	IM
Eu.SecSpec.862	Req	The IM shall define roles following least privilege principle.	IM
Eu.SecSpec.863	Req	The IM shall assign duties to roles.	IM
Eu.SecSpec.2878	Req	The IM shall assign duties to the user based on the roles.	IM
Eu.SecSpec.2879	Head	<b>2.2.5 M00066: Authorisation of SCI machine-to-machine communication</b>	
Eu.SecSpec.2880	Head	<b>2.2.5.1 General</b>	
Eu.SecSpec.2881	Info	Measure ID: M00066	--
Eu.SecSpec.2882	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• EfeS</li> <li>• TCS</li> <li>• ILS-Adapter</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.2883	Info	Threats: <ul style="list-style-type: none"> <li>• T 023 Unauthorised Access to IT Systems</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 032 Abuse of Authorisations</li> <li>• T 035 Coercion, Extortion or Corruption</li> </ul>	--
Eu.SecSpec.2884	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 1.2, SR 1.2 RE 1</li> <li>• SR 2.1, SR 2.1 RE 1, SR 2.1 RE 2</li> </ul>	--
Eu.SecSpec.2885	Req	The component shall only process PDI messages which have been received from the respective communication partner matching all its available identifiers.	All
Eu.SecSpec.2886	Req	If variant B or C is used, the component shall validate the identity of the expected SCI communication partner addressed by the PDI technical identifier using the common name of its TLS certificate which is used to establish the respective TLS connection(s).	All
Eu.SecSpec.2887	Req	If variant B or C is used, the component shall validate the identity of the expected SCI communication partner addressed by the PDI operational identifier using the common name of its TLS certificate which is used to establish the respective TLS connection(s).	All
Eu.SecSpec.2888	Req	If a PDI message is not processed due to a failed identifiers validation, the component shall terminate the SCI connection.	All
Eu.SecSpec.2889	Req	If a PDI message is not processed due to a failed identifiers validation, the EfeS component shall not re-establish the SCI connection until reboot.	All
Eu.SecSpec.2890	Info	The reboot of an EfeS can be triggered using SMI.	--
Eu.SecSpec.2891	Req	If a PDI message is not processed due to a failed identifiers validation, the EIL component shall not re-establish the SCI connection until commanded to re-enable the respective SCI communication.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2892	Req	If a PDI message is not processed due to a failed identifiers validation and variant B or C is used, the component shall terminate all respective TLS connections used by the SCI connection.	All
Eu.SecSpec.2893	Req	If a PDI message is not processed due to a failed identifiers validation and variant B or C is used, the EfeS component shall not re-establish all respective TLS connections used by the SCI connection until reboot.	All
Eu.SecSpec.2894	Req	If a PDI message is not processed due to a failed identifiers validation and variant B or C is used, the EIL component shall not re-establish all respective TLS connections used by the SCI connection until commanded to re-enable the respective SCI communication.	All
Eu.SecSpec.2895	Info	The MDM provides valid communication relations between technical and operational identifiers and the corresponding common name of the SCI TLS certificate of the communication partners.	--
Eu.SecSpec.864	Head	<b>2.3 Use Control (UC)</b>	
Eu.SecSpec.865	Head	<b>2.3.1 M00006: Alert personnel in case of detected unfavourable climatic conditions</b>	
Eu.SecSpec.2745	Head	<b>2.3.1.1 General</b>	
Eu.SecSpec.867	Info	Measure ID: M00006	--
Eu.SecSpec.868	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.872	Info	Threats: <ul style="list-style-type: none"><li>• T 02 Unfavourable Climate Conditions</li><li>• T 024 Destruction of Devices or Storage Media</li><li>• T 034 Attack</li></ul>	--
Eu.SecSpec.876	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SR 2.10</li></ul>	--
Eu.SecSpec.879	Req	The system shall track temperature.	All
Eu.SecSpec.2896	Req	The system shall track humidity.	All
Eu.SecSpec.2897	Req	The system shall track climate conditions, beside humidity and temperature.	All
Eu.SecSpec.2898	Req	The IM shall define climate conditions to be tracked.	IM
Eu.SecSpec.2899	Req	The IM shall define thresholds for alarms based on climatic conditions.	IM
Eu.SecSpec.2900	Req	If thresholds for climatic conditions are reached, the system shall send warnings via SSI-XX-SLOG.	All
Eu.SecSpec.2719	Head	<b>2.3.2 M00037: Security checks for personnel</b>	
Eu.SecSpec.2746	Head	<b>2.3.2.1 General</b>	
Eu.SecSpec.883	Info	Measure ID: M00037	--
Eu.SecSpec.884	Info	Affected SuC: <ul style="list-style-type: none"><li>• SCS</li></ul>	--
Eu.SecSpec.886	Info	Threats: <ul style="list-style-type: none"><li>• T 019 Disclosure of Sensitive Information</li><li>• T 030 Unauthorised Use or Administration of Devices and Systems</li><li>• T 041 Sabotage</li><li>• T 042 Social Engineering</li></ul>	--
Eu.SecSpec.891	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• None</li></ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.894	Req	The IM shall perform security checks for personnel which has access to classified devices.	IM
Eu.SecSpec.2901	Req	The IM shall perform security checks for personnel which has access to classified data.	IM
Eu.SecSpec.2902	Req	If suppliers or service providers have access to classified devices or data, the IM shall perform security checks for this personnel.	IM
Eu.SecSpec.2903	Req	The IM shall establish a classification scheme for devices.	IM
Eu.SecSpec.2904	Req	The IM shall establish a classification scheme for documents.	IM
Eu.SecSpec.2905	Req	The IM shall set up contractual agreements regarding security checks for service providers and suppliers.	IM
Eu.SecSpec.895	Info	Sensitive devices are inter alia: <ul style="list-style-type: none"> <li>• non-redundant management devices and systems</li> <li>• Potential single points of failure</li> <li>• Devices in the Network Operations Centre (NOC)</li> </ul>	--
Eu.SecSpec.899	Info	Sensitive information/data are inter alia: <ul style="list-style-type: none"> <li>• usage of management systems in case of misuse creating major disturbances.</li> <li>• confidential planning information</li> <li>• confidential configuration data</li> <li>• information allowing identifying weak points (e.g., information available to CERT) or single points of failures</li> </ul>	--
Eu.SecSpec.904	Head	<b>2.3.3 M00042: Dual control principle for administration</b>	
Eu.SecSpec.2747	Head	<b>2.3.3.1 General</b>	
Eu.SecSpec.906	Info	Measure ID: M00042	--
Eu.SecSpec.907	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.914	Info	Threats: <ul style="list-style-type: none"> <li>• T 022 Manipulation of Information</li> <li>• T 023 Unauthorised Access to IT Systems</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 031 Incorrect Use or Administration of Devices and Systems</li> <li>• T 032 Abuse of Authorisations</li> <li>• T 035 Coercion, Extortion or Corruption</li> <li>• T 041 Sabotage</li> <li>• T 044 Unauthorised Entry to Premises</li> <li>• T 046 Loss of Integrity of Sensitive Information</li> <li>• E 002 Inconsistent Configuration or Status Information</li> </ul>	--
Eu.SecSpec.925	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2906	Info	Dual control: more than one administrator is required to use a single function.	--
Eu.SecSpec.928	Req	The IM shall define critical functions which require the implementation of the dual control principle.	IM
Eu.SecSpec.2907	Req	The IM shall define rules which administrators are allowed to use the critical functions following the dual control principle.	IM
Eu.SecSpec.2908	Req	The IM shall define logging requirements for the usage of dual control principles.	IM
Eu.SecSpec.929	Head	<b>2.3.4 M00057: Analysis of administrator behaviour</b>	

ID	Type	Requirement	Valid for
Eu.SecSpec.2748	Head	<b>2.3.4.1 General</b>	
Eu.SecSpec.931	Info	Measure ID: M00057	--
Eu.SecSpec.932	Info	Affected SuC: <ul style="list-style-type: none"><li>EIL</li><li>EfeS</li><li>SCS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.937	Info	Threats: <ul style="list-style-type: none"><li>T 031 Incorrect Use or Administration of Devices and Systems</li><li>T 032 Abuse of Authorisations</li><li>T 035 Coercion, Extortion or Corruption</li></ul>	--
Eu.SecSpec.941	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.944	Req	The component shall track administration actions as logging data.	All
Eu.SecSpec.2909	Req	The component shall transmit logging data of administration actions to SSP via SSI-XX-SLOG.	All
Eu.SecSpec.945	Head	<b>2.4 System Integrity (SI)</b>	
Eu.SecSpec.946	Head	<b>2.4.1 M00021: Protect integrity of devices</b>	
Eu.SecSpec.2749	Head	<b>2.4.1.1 General</b>	
Eu.SecSpec.948	Info	Measure ID: M00021	--
Eu.SecSpec.949	Info	Affected SuC: <ul style="list-style-type: none"><li>EIL</li><li>MDM</li><li>SSP</li><li>EfeS</li><li>SCS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.955	Info	Threats: <ul style="list-style-type: none"><li>T 015 Eavesdropping</li><li>T 019 Disclosure of Sensitive Information</li><li>T 021 Manipulation of Hardware or Software</li><li>T 035 Coercion, Extortion or Corruption</li><li>T 039 Malicious Software</li><li>T 042 Social Engineering</li><li>T 044 Unauthorised Entry to Premises</li><li>E 001 Black mail</li><li>E 002 Inconsistent Configuration or Status Information</li></ul>	--
Eu.SecSpec.965	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>SR 3.4, SR 3.4 RE 1</li></ul>	--
Eu.SecSpec.968	Info	It needs to be considered that a system in some cases cannot detect by itself that it has been compromised. Only surrounding systems might be able to assume/suspect/suppose/detect that another system may be compromised.	--
Eu.SecSpec.970	Req	The component shall provide the capability to protect the hardware integrity.	All
Eu.SecSpec.971	Req	The component shall provide the capability to protect the software integrity.	All
Eu.SecSpec.972	Req	The component shall provide the capability to protect the configuration integrity.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.976	Req	The component shall use automatic reoccurring checks to monitor the integrity.	All
Eu.SecSpec.2910	Req	The component shall provide the capability to trigger integrity checks via SMI.	All
Eu.SecSpec.2911	Req	The component shall implement integrity checks which do not affect operational availability.	All
Eu.SecSpec.977	Head	<b>2.4.1.2 EfeS, SCS, ILS-Adapter</b>	
Eu.SecSpec.978	Req	The component shall check integrity of hardware before it is used at start up.	All
Eu.SecSpec.2912	Req	The component shall check integrity of software before it is used at start up.	All
Eu.SecSpec.2913	Req	The component shall check integrity of configuration before it is used at start up.	All
Eu.SecSpec.2914	Req	The component shall terminate its operation if any integrity check at start up failed.	All
Eu.SecSpec.2915	Info	This can be performed using e.g., secure boot and is implemented according to IEC 62443-4-2 HDR 3.14 or NDR 3.14.	--
Eu.SecSpec.2916	Req	The supplier shall provide signed software.	All
Eu.SecSpec.2917	Req	The component shall authenticate all hardware-separated subcomponents.	All
Eu.SecSpec.2918	Req	The component shall check authorisation of the data flow from and to hardware-separated subcomponents.	All
Eu.SecSpec.2919	Req	The component shall ensure integrity of the data flow from and to hardware-separated subcomponents.	All
Eu.SecSpec.984	Head	<b>2.4.2 M00023: Cryptographic integrity protection</b>	
Eu.SecSpec.2750	Head	<b>2.4.2.1 General</b>	
Eu.SecSpec.986	Info	Measure ID: M00023	--
Eu.SecSpec.987	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• EfeS</li><li>• ILS-Adapter</li><li>• TCS</li><li>• RBC</li></ul>	--
Eu.SecSpec.994	Info	Threats: <ul style="list-style-type: none"><li>• T 014 Interception of Information / Espionage</li><li>• T 019 Disclosure of Sensitive Information</li><li>• T 022 Manipulation of Information</li><li>• T 030 Unauthorised Use or Administration of Devices and Systems</li><li>• T 035 Coercion, Extortion or Corruption</li><li>• T 043 Replaying Messages</li><li>• T 046 Loss of Integrity of Sensitive Information</li><li>• E 001 Black mail</li></ul>	--
Eu.SecSpec.1003	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SR 3.1, SR 3.1 RE 1</li><li>• SR 3.8, SR 3.8 RE 1, SR 3.8 RE 2</li><li>• SR 3.9</li><li>• SR 4.3</li></ul>	--
Eu.SecSpec.1013	Req	The component shall protect the integrity of data using state of the art cryptographic methods.	All
Eu.SecSpec.2920	Req	The component shall detect loss of integrity of data using state of the art cryptographic methods.	All
Eu.SecSpec.1014	Req	The component shall be able to update cryptographic methods used for integrity protection without affecting safety certification.	All



ID	Type	Requirement	Valid for
Eu.SecSpec.1029	Head	<b>2.4.2.2 Network-specific Measure / Data (information) in transit</b>	
Eu.SecSpec.1009	Req	The component shall protect the integrity of data in transit.	All
Eu.SecSpec.2921	Info	The integrity of data in transit can be protected	--
Eu.SecSpec.1010	Info	• by application/service (OSI layer 7, processual end-to-end)	--
Eu.SecSpec.1011	Info	• or by communication endpoint within application/service (communication end-to-end)	--
Eu.SecSpec.1012	Info	• or by subsystem communication system's endpoint (communication device end-to-end)	--
Eu.SecSpec.1016	Req	The component shall ensure mutual authentication.	All
Eu.SecSpec.2922	Req	The EULYNX field element Subsystem (EfeS) shall support Variant A and either Variant B or C.	All
Eu.SecSpec.1031	Req	If variant B or C is used, the component shall use TLS for cryptographic integrity protection.	All
Eu.SecSpec.2923	Info	Details on the TLS requirements are provided in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.SecSpec.2812	Req	If variant B or C is used, the component shall support periodic re-authentication during an active session for the TLS connection.	All
Eu.SecSpec.2924	Req	If variant B or C is used, the component shall support separate re-authentication per TLS connection.	All
Eu.SecSpec.2925	Info	Separate re-authentication may ensure that at least one TLS connection stays active - also if re-authentication fails for availability reasons.	--
Eu.SecSpec.1018	Req	If variant B or C is used, the component shall only provide integrity-only ciphers for connections without a required confidentiality protection.	All
Eu.SecSpec.2926	Req	If variant B or C is used, the component shall provide the capability to activate and deactivate integrity-only ciphers in a secure manner.	All
Eu.SecSpec.2927	Req	If variant B or C is used, the IM shall define which connection requires data confidentiality.	IM
Eu.SecSpec.2928	Info	The risk analysis recommends data confidentiality for specific connections in Measure M00024.	--
Eu.SecSpec.1034	Head	<b>2.4.2.3 Data (information) at rest</b>	
Eu.SecSpec.1036	Req	The component shall protect the integrity of log data at rest using hash algorithms according to Eu.Doc.115.	All
Eu.SecSpec.2929	Req	The component shall protect the integrity of juridical recording data at rest using hash algorithms according to Eu.Doc.115.	All
Eu.SecSpec.2930	Req	The component shall protect the integrity of software updates at rest using hash algorithms according to Eu.Doc.115.	All
Eu.SecSpec.2931	Req	The component shall protect the integrity of configuration data at rest using hash algorithms according to Eu.Doc.115.	All
Eu.SecSpec.2932	Req	The SSP-XX-BKP Service shall protect the integrity of backup data at rest using hash algorithms according to Eu.Doc.115.	All
Eu.SecSpec.2933	Req	The component shall protect the integrity of all cryptographic keys.	All
Eu.SecSpec.1037	Head	<b>2.4.3 M00028: Protection of software and configuration updates</b>	
Eu.SecSpec.2751	Head	<b>2.4.3.1 General</b>	
Eu.SecSpec.1039	Info	Measure ID: M00028	--
Eu.SecSpec.1040	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1047	Info	Threats: <ul style="list-style-type: none"> <li>• T 014 Interception of Information / Espionage</li> <li>• T 019 Disclosure of Sensitive Information</li> <li>• T 020 Information or Products from an Unreliable Source</li> <li>• T 021 Manipulation of Hardware or Software</li> <li>• T 043 Replaying Messages</li> <li>• T 046 Loss of Integrity of Sensitive Information</li> <li>• E 002 Inconsistent Configuration or Status Information</li> </ul>	--
Eu.SecSpec.1055	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 3.4</li> </ul>	--
Eu.SecSpec.1058	Req	The component shall be able to check the integrity and authenticity of a supplied software.	All
Eu.SecSpec.2934	Req	The supplier shall provide a hash of software updates signed with the suppliers private key.	All
Eu.SecSpec.2935	Req	The supplier shall use hash algorithms for the integrity protection of software updates according to Eu.Doc.115.	All
Eu.SecSpec.1059	Req	The supplier shall apply SM 6, SM 7, SM 8 from IEC 62443-4-1 for the development and signing process.	All
Eu.SecSpec.1061	Req	The storage media containing software and configuration updates shall provide a visible identifier.	All
Eu.SecSpec.2936	Req	If configuration data is provided using storage media, the component shall be able to check the integrity of configuration data.	All
Eu.SecSpec.2937	Req	If configuration data is provided using storage media, the IM or supplier shall provide a hash of configuration data signed with the corresponding private key.	All
Eu.SecSpec.2938	Req	If configuration data is provided using storage media, the IM or supplier shall use hash algorithms for the integrity protection of configuration data according to Eu.Doc.115.	All
Eu.SecSpec.2939	Req	The IM or supplier shall track the location of storage media containing software and configuration updates.	All
Eu.SecSpec.1065	Head	<b>2.4.4 M00052: Separation of safety and security</b>	
Eu.SecSpec.2752	Head	<b>2.4.4.1 General</b>	
Eu.SecSpec.1067	Info	Measure ID: M00052	--
Eu.SecSpec.1068	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• EfeS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1073	Info	Threats: <ul style="list-style-type: none"> <li>• T 028 Software Vulnerabilities or Errors</li> </ul>	--
Eu.SecSpec.1075	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.1078	Req	The component shall be designed in a way that altering the security system is not compromising or altering the safety of the system.	All
Eu.SecSpec.1079	Req	The component shall provide the ability to update the changeable security functionalities without affecting safety approvals.	All
Eu.SecSpec.1080	Info	The separation can be implemented using different devices or using kernel-level separation.	--
Eu.SecSpec.1121	Head	<b>2.5 Data Confidentiality (DC)</b>	
Eu.SecSpec.1122	Head	<b>2.5.1 M00019: Limitation of security-relevant emissions</b>	
Eu.SecSpec.2755	Head	<b>2.5.1.1 General</b>	--
Eu.SecSpec.1124	Info	Measure ID: M00019	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1125	Info	Affected SuC: <ul style="list-style-type: none"><li>EfeS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.1128	Info	Threats: <ul style="list-style-type: none"><li>T 013 Intercepting Compromising Emissions</li></ul>	--
Eu.SecSpec.1130	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.1133	Req	The component shall limit electro-magnetic emission containing information on private cryptographic keys.	All
Eu.SecSpec.1135	Info	Military grade measure (like TEMPEST) may not be required.	--
Eu.SecSpec.1136	Head	<b>2.5.2 M00020: Protection of private keys</b>	
Eu.SecSpec.2756	Head	<b>2.5.2.1 General</b>	
Eu.SecSpec.1138	Info	Measure ID: M00020	--
Eu.SecSpec.1139	Info	Affected SuC: <ul style="list-style-type: none"><li>EfeS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.1142	Info	Threats: <ul style="list-style-type: none"><li>T 013 Intercepting Compromising Emissions</li><li>T 023 Unauthorised Access to IT Systems</li></ul>	--
Eu.SecSpec.1145	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>SR 1.5 RE 1</li><li>SR 1.9 RE1</li><li>SR 4.3</li></ul>	--
Eu.SecSpec.2940	Req	The component shall prevent unauthorized access to private keys used in public-private key cryptography using a dedicate hardware security module (HSM) or trusted execution environment (TEE).	All
Eu.SecSpec.2941	Req	The component shall prevent unauthorized access to keys used in symmetric cryptography using a dedicate hardware security module (HSM) or trusted execution environment (TEE).	All
Eu.SecSpec.485	Req	The component shall generate keys on the component itself.	All
Eu.SecSpec.3124	Req	The component shall only store generated private keys on the component itself.	All
Eu.SecSpec.486	Req	If a component has a HSM (Hardware Security Module) the component shall generate keys on the HSM itself.	All
Eu.SecSpec.2943	Req	If a component has a HSM (Hardware Security Module) the component shall store private keys on the HSM itself.	All
Eu.SecSpec.2944	Req	If a component has a TEE (Trusted Execution Environment) the component shall generate keys on the TEE itself.	All
Eu.SecSpec.2945	Req	If a component has a TEE (Trusted Execution Environment) the component shall store private keys on the TEE itself.	All
Eu.SecSpec.488	Info	TPM (Trusted Platform Modules) version 1.2 is considered to be an outdated solution.	--
Eu.SecSpec.1152	Req	The HSM must be updateable with feasible effort to be conformant over time.	All
Eu.SecSpec.2946	Req	The TEE must be updateable with feasible effort to be conformant over time.	All
Eu.SecSpec.2947	Info	A software based "HSM" (hardware security module) or "TEE" (trusted execution environment) is acceptable if included in a separation kernel setup with measure to ensure system integrity. Any protective measure must comply with national regulation and recommendations on use of cryptographic methods.	--
Eu.SecSpec.1153	Head	<b>2.5.3 M00024: Data confidentiality</b>	
Eu.SecSpec.2757	Head	<b>2.5.3.1 General</b>	

ID	Type	Requirement	Valid for
Eu.SecSpec.1155	Info	Measure ID: M00024	--
Eu.SecSpec.1156	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• ILS-Adapter</li> <li>• SCS</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.1164	Info	Threats: <ul style="list-style-type: none"> <li>• T 013 Intercepting Compromising Emissions</li> <li>• T 014 Interception of Information / Espionage</li> <li>• T 015 Eavesdropping</li> <li>• T 019 Disclosure of Sensitive Information</li> <li>• T 022 Manipulation of Information</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 042 Social Engineering</li> <li>• T 041 Sabotage</li> <li>• T 043 Replaying Messages</li> <li>• T 044 Unauthorised Entry to Premises</li> <li>• T 046 Loss of Integrity of Sensitive Information</li> <li>• E 002 Inconsistent Configuration or Status Information</li> </ul>	--
Eu.SecSpec.1177	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 3.9</li> <li>• SR 4.1, SR 4.1 RE 1</li> <li>• SR 4.2, SR 4.2 RE 1</li> <li>• SR 4.3</li> </ul>	--
Eu.SecSpec.1182	Req	The component shall protect the confidentiality of data using state of the art cryptographic methods.	All
Eu.SecSpec.1184	Req	The component shall be able to update cryptographic methods used for confidentiality protection without affecting safety certification.	All
Eu.SecSpec.1188	Info	If integrity protection is required as well, a technical solution combining integrity and confidentiality is preferred.	--
Eu.SecSpec.1186	Req	The component shall implement encryption using encrypt then MAC (EtM).	All
Eu.SecSpec.2948	Info	For example EtM is used in TLS 1.3 which is using Authenticated Encryption with Associated Data (AEAD). This ensures decryption is done only on data which doesn't have a broken integrity and has a valid origin.	--
Eu.SecSpec.1191	Head	<b>2.5.3.2 Data in transit</b>	
Eu.SecSpec.1195	Req	The component shall protect confidentiality of configuration data in transit on SMI.	All
Eu.SecSpec.2949	Req	The component shall protect confidentiality of software update data in transit on SMI.	All
Eu.SecSpec.1196	Req	The component shall protect confidentiality of diagnostic data in transit on SDI.	All
Eu.SecSpec.1198	Req	The component shall protect confidentiality of security logging data in transit on SSI.	All
Eu.SecSpec.1199	Req	The SCS component shall protect confidentiality of SCS management plane.	All
Eu.SecSpec.2950	Info	As the management plane of the SCS shall be encrypted, this encryption protects the basic functionality of the SCS, hence its availability and quality of service. It does not protect any confidentiality requirements of the user of the transport network service.	--
Eu.SecSpec.1200	Req	The component shall protect confidentiality of remote management data in transit.	All
Eu.SecSpec.1201	Info	The confidentiality of data in transit can be protected	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1202	Info	• by end users (processual end-to-end)	--
Eu.SecSpec.1203	Info	• or by end users (communication endpoint-to-endpoint)	--
Eu.SecSpec.1204	Info	• or by subsystem communication system (communication end-to-end)	--
Eu.SecSpec.2951	Req	The component shall ensure mutual authentication.	All
Eu.SecSpec.1205	Req	If variant B or C is used, the component shall use TLS for cryptographic confidentiality protection.	All
Eu.SecSpec.2952	Info	Details on the TLS requirements are provided in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.SecSpec.2811	Req	If variant B or C is used, the component shall support periodic re-authentication during an active session for the TLS connection.	All
Eu.SecSpec.2953	Req	If variant B or C is used, the component shall support separate re-authentication per TLS connection.	All
Eu.SecSpec.1206	Info	See also requirements for OPC-UA and SNMP in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.SecSpec.1211	Head	<b>2.5.3.3 Data at rest</b>	
Eu.SecSpec.1214	Req	The component shall protect confidentiality of configuration data at rest.	All
Eu.SecSpec.1216	Req	The component shall protect confidentiality of private keys at rest.	All
Eu.SecSpec.1217	Req	The component shall protect confidentiality of symmetric keys at rest.	All
Eu.SecSpec.1218	Req	The component shall protect confidentiality of recovery keys at rest.	All
Eu.SecSpec.1219	Info	Encrypt storage according to the requirements for encryption for data at rest in the EULYNX Security Parameter Specification [Eu.Doc.115].	--
Eu.SecSpec.2737	Req	The IM shall require and establish procedures to securely purge data right after last usage for data stored on mobile or removable media.	IM
Eu.SecSpec.1220	Head	<b>2.5.3.4 Data in process</b>	
Eu.SecSpec.1222	Info	For software development, methods may be used which take into account the protection of the confidentiality of data in process against an attacker according to the SL-T definition. It is recommended that corresponding assessment and resulting decisions for software design and technologies be documented.	--
Eu.SecSpec.1223	Head	<b>2.6 Restricted Data Flow (RDF)</b>	
Eu.SecSpec.1224	Head	<b>2.6.1 M00051: Network segmentation</b>	
Eu.SecSpec.2758	Head	<b>2.6.1.1 General</b>	--
Eu.SecSpec.1226	Info	Measure ID: M00051	--
Eu.SecSpec.1227	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.1235	Info	Threats: <ul style="list-style-type: none"> <li>• T 028 Software Vulnerabilities or Errors</li> <li>• T 039 Malicious Software</li> <li>• T 040 Denial of Service</li> <li>• T 043 Replaying Messages</li> <li>• E 002 Inconsistent Configuration or Status Information</li> </ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1241	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>SR 5.1</li></ul>	--
Eu.SecSpec.1244	Req	The component shall have the capability for network segmentation according to IEC 62443-3-3 SR 5.1 (RE 1 excluded) and IEC 62443-4-2 CR 5.1	All
Eu.SecSpec.2954	Req	The subsystem communication system shall implement network segmentation according to IEC 62443-3-3 SR 5.1 (RE 1 excluded)	All
Eu.SecSpec.1246	Info	See also the Specification of Point of Service-Signalling [EU.Doc.100].	--
Eu.SecSpec.1247	Head	<b>2.6.2 M00053: Firewall and intrusion detection</b>	
Eu.SecSpec.2759	Head	<b>2.6.2.1 General</b>	
Eu.SecSpec.1249	Info	Measure ID: M00053	--
Eu.SecSpec.1250	Info	Affected SuC: <ul style="list-style-type: none"><li>EIL</li><li>MDM</li><li>SSP</li><li>EfeS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.1255	Info	Threats: <ul style="list-style-type: none"><li>T 028 Software Vulnerabilities or Errors</li><li>T 039 Malicious Software</li><li>T 040 Denial of Service</li></ul>	--
Eu.SecSpec.1259	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>SR 3.2, SR 3.2 RE 1</li><li>SR 5.2, SR 5.2 RE 1</li></ul>	--
Eu.SecSpec.1265	Req	The filter shall block unknown OSI layer 2-4 protocols.	All
Eu.SecSpec.1266	Req	The filter shall block OSI layer 2-4 protocols considered with unacceptable security risks.	All
Eu.SecSpec.2955	Req	The filter shall block OSI layer 2-4 protocol functions considered with unacceptable security risks.	All
Eu.SecSpec.1267	Req	The filter shall block connections from unknown source addresses.	All
Eu.SecSpec.1268	Req	The filter shall block connections to protected destination addresses.	All
Eu.SecSpec.1269	Req	The filter shall block connections from internal source addresses which should not access other networks.	All
Eu.SecSpec.1270	Req	The filter shall block encrypted connections which do not match the encryptions policies	All
Eu.SecSpec.1271	Req	The filter shall block connections with required encryption which are not encrypted	All
Eu.SecSpec.1273	Info	Some of these functionalities might be implemented using Software Defined Networks (SDN).	--
Eu.SecSpec.1275	Info	The integration of firewall and IDS is defined in the EULYNX Security Concept [Eu.Doc.15].	--
Eu.SecSpec.1277	Head	<b>2.6.2.2 EfeS and ILS-Adapter</b>	
Eu.SecSpec.1278	Req	The component's filter shall filter incoming network traffic.	All
Eu.SecSpec.1279	Head	<b>2.6.2.3 EIL, MDM and SSP</b>	
Eu.SecSpec.1280	Req	The filter shall block OSI layer 5-7 packets which have not been whitelisted by the IM.	All
Eu.SecSpec.3130	Req	The IM shall define the whitelist to be used by the filter.	IM
Eu.SecSpec.1281	Info	Automatic reaction mechanisms, like Intrusion Prevention System (IPS) or Security Orchestration, Automation and Response (SOAR) shall only be used considering availability aspects.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2956	Req	The filter of system EIL shall filter incoming network traffic as self protection at the security zone border.	All
Eu.SecSpec.2957	Req	The filter of system MDM shall filter incoming network traffic as self protection at the security zone border.	All
Eu.SecSpec.2958	Req	The filter of system SSP shall filter incoming network traffic as self protection at the security zone border.	All
Eu.SecSpec.1282	Head	<b>2.7 Timely Response to Events (TRE)</b>	
Eu.SecSpec.1283	Head	<b>2.7.1 M00022: Central logging and event management</b>	
Eu.SecSpec.2760	Head	<b>2.7.1.1 General</b>	
Eu.SecSpec.1285	Info	Measure ID: M00022	--
Eu.SecSpec.1286	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.1293	Info	Threats: <ul style="list-style-type: none"> <li>• T 014 Interception of Information / Espionage</li> <li>• T 019 Disclosure of Sensitive Information</li> <li>• T 022 Manipulation of Information</li> <li>• T 026 Malfunction of Devices or Systems</li> <li>• T 028 Software Vulnerabilities or Errors</li> <li>• T 029 Violation of Laws or Regulations</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 031 Incorrect Use or Administration of Devices and Systems</li> <li>• T 032 Abuse of Authorisations</li> <li>• T 035 Coercion, Extortion or Corruption</li> <li>• T 037 Repudiation of Actions</li> <li>• T 039 Malicious Software</li> <li>• T 040 Denial of Service</li> <li>• T 042 Social Engineering</li> <li>• T 043 Replaying Messages</li> <li>• T 044 Unauthorised Entry to Premises</li> <li>• T 046 Loss of Integrity of Sensitive Information</li> </ul>	--
Eu.SecSpec.1311	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 1.13</li> <li>• SR 2.8, SR 2.8 RE 1</li> <li>• SR 2.9, SR 2.9 RE 1</li> <li>• SR 2.10</li> <li>• SR 2.11, SR 2.11 RE 1</li> <li>• SR 2.12</li> <li>• SR 3.2, SR 3.2 RE 2</li> <li>• SR 3.9</li> <li>• SR 6.1, SR 6 RE 1</li> <li>• SR 6.2</li> <li>• SR 7.6 RE 1</li> </ul>	--
Eu.SecSpec.1324	Info	EULYNX uses the term "logging" dedicated only to tapped network traffic by the MDM. The security documents use the term of logging for diagnostic or monitoring purposes.	--
Eu.SecSpec.1326	Req	The IM shall ensure a centrally managed system-wide audit trail is implemented according to SR 2.8 RE 1 from IEC 62443-3-3.	IM
Eu.SecSpec.2959	Req	The SIEM shall have at least access to the system-wide audit trail.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2960	Req	The component shall implement CR 2.8 from IEC 62443-4-2.	All
Eu.SecSpec.2961	Req	The component shall provide log data to the SSP-SLOG service via SSI-XX-SLOG.	All
Eu.SecSpec.1328	Req	The component shall protect log files using read only access rights for users and file access rules.	All
Eu.SecSpec.2962	Req	The component shall ensure availability of the log information.	All
Eu.SecSpec.2963	Info	Logging program may be restricted to only append to files.	--
Eu.SecSpec.1329	Req	The component shall protect log data at least according to M00023 and M00024.	All
Eu.SecSpec.1330	Req	The component shall use synchronized time for log time stamps.	All
Eu.SecSpec.2964	Req	The component shall synchronize using SDI time synchronization interface.	All
Eu.SecSpec.1331	Req	If the MDM is not used to distribute security settings, the component shall provide machine-readable reports of the currently deployed security settings according to IEC 62443 SR 7.6 RE 1.	All
Eu.SecSpec.2965	Req	If the MDM is used to distribute security settings, the MDM shall provide machine-readable reports of the currently deployed security settings according to IEC 62443 SR 7.6 RE 1 for all components.	All
Eu.SecSpec.1332	Head	<b>2.7.1.1.1 MDM</b>	
Eu.SecSpec.2966	Req	If the service function diagnostic collector is not working as intended, the MDM shall issue an alarm.	All
Eu.SecSpec.1338	Req	The IM must implement processes to respond to alarms of the MDM system.	IM
Eu.SecSpec.1339	Head	<b>2.7.1.1.2 SCS</b>	
Eu.SecSpec.1341	Req	The SCS shall implement diagnostic and monitoring logging capabilities.	All
Eu.SecSpec.1343	Info	Additional network telemetry can be gathered from involved network routers or switches for security and network anomaly detection purposes based on standard like NetFlow (RFC 3954) or IPFIX (RFC 3917). The risks of using network security and network anomaly detection tools have to be analysed individually by the IM, to respect the specific network setup (design and operation).	--
Eu.SecSpec.1428	Head	<b>2.7.1.2 General logging requirements</b>	
Eu.SecSpec.1430	Req	The component shall store log data until the transfer is acknowledged by the SSI-XX-SLOG interface.	All
Eu.SecSpec.2967	Req	The component shall store log data on a non-volatile memory.	All
Eu.SecSpec.1434	Req	The component shall store untransferred log data for eight hours.	All
Eu.SecSpec.2968	Req	The component shall store log data of 10000 untransferred log entries.	All
Eu.SecSpec.2969	Req	If the storage capacity is exceeded, the component shall overwrite the oldest entry first.	All
Eu.SecSpec.1502	Head	<b>2.7.2 M00040: Network monitoring</b>	
Eu.SecSpec.2762	Head	<b>2.7.2.1 General</b>	
Eu.SecSpec.1504	Info	Measure ID: M00040	--
Eu.SecSpec.1505	Info	Affected SuC: <ul style="list-style-type: none"><li>• SCS</li><li>• TCS</li><li>• RBC</li></ul>	--
Eu.SecSpec.1509	Info	Threats: <ul style="list-style-type: none"><li>• T 09 Failure or Disruption of Communication Networks</li><li>• T 010 Failure or Disruption of Main Supply</li><li>• T 036 Identity Theft</li><li>• T 040 Denial of Service</li><li>• T 044 Unauthorised Entry to Premises</li></ul>	--



ID	Type	Requirement	Valid for
Eu.SecSpec.1515	Info	Reference to IEC 62443: • SR 7.1 RE 1	--
Eu.SecSpec.1519	Req	The network system shall monitor network utilization.	All
Eu.SecSpec.2970	Info	Network utilization monitoring includes network load, QoS, and congestion.	--
Eu.SecSpec.1520	Req	The network system shall send alerts regarding critical network utilization to responsible personnel.	All
Eu.SecSpec.1545	Head	<b>2.7.3 M00059: Local log storage and juridical recording</b>	
Eu.SecSpec.2764	Head	<b>2.7.3.1 General</b>	
Eu.SecSpec.1547	Info	Measure ID: M00059	--
Eu.SecSpec.1548	Info	Affected SuC: • EfeS • SCS • ILS-Adapter	--
Eu.SecSpec.1552	Info	Threats: • T 037 Repudiation of Actions	--
Eu.SecSpec.1554	Info	Reference to IEC 62443: • SR 2.12 • SR 3.9 • SR 6.1	--
Eu.SecSpec.1560	Req	The component shall store juridical recordings according to regulatory requirements.	All
Eu.SecSpec.1563	Head	<b>2.8 Resource Availability (RA)</b>	
Eu.SecSpec.1564	Head	<b>2.8.1 M00007: Highly available and protected air conditioning</b>	
Eu.SecSpec.2765	Head	<b>2.8.1.1 General</b>	
Eu.SecSpec.1566	Info	Measure ID: M00007	--
Eu.SecSpec.1567	Info	Affected SuC: • EIL • MDM • SSP	--
Eu.SecSpec.1570	Info	Threats: • T 02 Unfavourable Climate Conditions • T 024 Destruction of Devices or Storage Media • T 034 Attack	--
Eu.SecSpec.1574	Info	Reference to IEC 62443: • None	--
Eu.SecSpec.1577	Req	The air conditioning system shall provide climatic conditions required to fulfil the availability requirements of the EIL.	All
Eu.SecSpec.2971	Req	The air conditioning system shall provide climatic conditions required to fulfil the availability requirements of the MDM.	All
Eu.SecSpec.2972	Req	The air conditioning system shall provide climatic conditions required to fulfil the availability requirements of the SSP.	All
Eu.SecSpec.2973	Req	The air conditioning system shall report system failures to responsible personnel.	All
Eu.SecSpec.2974	Req	The air conditioning system shall be physically protected.	All
Eu.SecSpec.1578	Head	<b>2.8.2 M00012: Network resilience against single point of failure</b>	

ID	Type	Requirement	Valid for
Eu.SecSpec.2766	Head	<b>2.8.2.1 General</b>	
Eu.SecSpec.1580	Info	Measure ID: M00012	--
Eu.SecSpec.1581	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.1589	Info	Threats: <ul style="list-style-type: none"> <li>• T 07 Major Events in the Environment</li> <li>• T 09 Failure or Disruption of Communication Networks</li> <li>• T 010 Failure or Disruption of Main Supply</li> <li>• T 024 Destruction of Devices or Storage Media</li> <li>• T 034 Attack</li> <li>• T 039 Malicious Software</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.1597	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.1600	Req	The network shall provide fault tolerant disjoint paths.	All
Eu.SecSpec.2975	Info	Fault tolerance depends on potential negative impact on railway operation.	--
Eu.SecSpec.1602	Head	<b>2.8.2.2 SCS</b>	
Eu.SecSpec.1606	Req	If the network is in a degraded state, the network management plane shall provide essential functionality.	All
Eu.SecSpec.1607	Req	If the network is in a degraded state, the network access control shall provide essential functionality.	All
Eu.SecSpec.1614	Head	<b>2.8.3 M00013: Emergency Power Supply</b>	
Eu.SecSpec.2767	Head	<b>2.8.3.1 General</b>	
Eu.SecSpec.1616	Info	Measure ID: M00013	--
Eu.SecSpec.1617	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1623	Info	Threats: <ul style="list-style-type: none"> <li>• T 08 Failure or Disruption of the Power Supply</li> <li>• T 010 Failure or Disruption of Main Supply</li> <li>• T 034 Attack</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.1628	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 7.5</li> </ul>	--
Eu.SecSpec.1631	Req	The component shall maintain a secure state while switching to an emergency power supply according to IEC 62443 SR 7.5.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2976	Req	The power supply shall be physically protected.	All
Eu.SecSpec.1632	Head	<b>2.8.3.2 EIL</b>	
Eu.SecSpec.1633	Req	The EIL shall use an uninterruptible power supply.	All
Eu.SecSpec.2977	Req	The EIL shall use a redundant power supply.	All
Eu.SecSpec.2978	Req	The EIL shall use an emergency power supply.	All
Eu.SecSpec.2979	Req	The auxiliary systems of the EIL shall use an emergency power supply.	All
Eu.SecSpec.2980	Info	Auxiliary systems of the EIL include climate control and flood protection	--
Eu.SecSpec.1654	Head	<b>2.8.4 M00030: Backup of device data</b>	
Eu.SecSpec.2769	Head	<b>2.8.4.1 General</b>	--
Eu.SecSpec.1656	Info	Measure ID: M00030	--
Eu.SecSpec.1657	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1663	Info	Threats: <ul style="list-style-type: none"> <li>• T 016 Theft of Devices, Storage Media and Documents</li> <li>• T 017 Loss of Devices, Storage Media and Documents</li> <li>• T 024 Destruction of Devices or Storage Media</li> <li>• T 025 Failure of Devices or Systems</li> <li>• T 034 Attack</li> <li>• T 035 Coercion, Extortion or Corruption</li> <li>• T 041 Sabotage</li> <li>• T 042 Social Engineering</li> <li>• T 044 Unauthorised Entry to Premises</li> <li>• T 045 Data Loss</li> <li>• E 001 Black mail</li> </ul>	--
Eu.SecSpec.1675	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 7.3, SR 7.3 RE 1, SR 7.3 RE 2</li> </ul>	--
Eu.SecSpec.1679	Req	If an MDM is used, a backup of the MDM configuration, the configuration data of the devices managed by the MDM and the logging/diagnostic data saved by the MDM shall be done.	All
Eu.SecSpec.1685	Info	Relevant configuration data and software is distributed via the MDM. Hence this service is used to perform the backup centralized.	--
Eu.SecSpec.2981	Req	The MDM shall perform backups for the configuration data of the MDM.	All
Eu.SecSpec.2982	Req	The MDM shall perform backups for the configuration data of the EIL.	All
Eu.SecSpec.2983	Req	The MDM shall perform backups for the configuration data of the EfeS.	All
Eu.SecSpec.2984	Req	The MDM shall perform backups for the configuration data of the ILS-Adapter.	All
Eu.SecSpec.2985	Req	The MDM shall perform backup processes using SSP-BKP service.	All
Eu.SecSpec.2986	Req	The MDM shall perform backup restore processes using SSP-BKP service.	All
Eu.SecSpec.2987	Req	The MDM shall use SSI-XX-BKP interface to connect to SSP-BKP service.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2988	Req	The SSP shall perform backups for data relevant for operational availability.	All
Eu.SecSpec.2989	Req	The SSP shall perform backup processes using SSP-BKP service.	All
Eu.SecSpec.2990	Req	The SSP shall perform backup restore processes using SSP-BKP service.	All
Eu.SecSpec.2991	Req	The SSP shall use SSI-XX-BKP interface to connect to SSP-BKP service.	All
Eu.SecSpec.1700	Head	<b>2.8.5 M00033: Spare parts</b>	
Eu.SecSpec.2771	Head	<b>2.8.5.1 General</b>	--
Eu.SecSpec.1702	Info	Measure ID: M00033	--
Eu.SecSpec.1703	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1709	Info	Threats: <ul style="list-style-type: none"> <li>• T 016 Theft of Devices, Storage Media and Documents</li> <li>• T 017 Loss of Devices, Storage Media and Documents</li> <li>• T 024 Destruction of Devices or Storage Media</li> <li>• T 034 Attack</li> <li>• T 041 Sabotage</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.1716	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.1719	Req	The IM shall define requirements for the availability of spare parts considering security related disturbances in the supply chain.	IM
Eu.SecSpec.1722	Head	<b>2.8.6 M00039: System hardening</b>	
Eu.SecSpec.2772	Head	<b>2.8.6.1 General</b>	--
Eu.SecSpec.1724	Info	Measure ID: M00039	--
Eu.SecSpec.1725	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1731	Info	Threats: <ul style="list-style-type: none"> <li>• T 020 Information or Products from an Unreliable Source</li> <li>• T 022 Manipulation of Information</li> <li>• T 046 Loss of Integrity of Sensitive Information</li> </ul>	--
Eu.SecSpec.1735	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 1.7</li> <li>• SR 2.3</li> <li>• SR 7.7</li> </ul>	--
Eu.SecSpec.1740	Req	The IM shall define system hardening measures.	IM

ID	Type	Requirement	Valid for
Eu.SecSpec.2992	Req	The supplier shall implement system hardening measures.	All
Eu.SecSpec.2993	Req	The supplier shall document the implementation of system hardening measures.	All
Eu.SecSpec.1744	Req	The supplier shall remove accounts which are not required for operation.	All
Eu.SecSpec.1745	Req	The supplier shall deactivate unused interfaces.	All
Eu.SecSpec.2994	Info	Unused interfaces to check include amongst others network, USB, WLAN, serial, Bluetooth and NFC.	--
Eu.SecSpec.2995	Req	The supplier shall deactivate unused network services.	All
Eu.SecSpec.1746	Req	The supplier shall deactivate interfaces which are not specified in EULYNX.	All
Eu.SecSpec.2996	Req	The IM shall define which non-EUYLNX interfaces can be activated by the supplier.	IM
Eu.SecSpec.1748	Req	The supplier shall remove unnecessary drivers.	All
Eu.SecSpec.1749	Req	The supplier shall deactivate non-essential services.	All
Eu.SecSpec.1822	Head	<b>2.8.7 M00060: Protection against Denial of Service (DoS)</b>	
Eu.SecSpec.2777	Head	<b>2.8.7.1 General</b>	--
Eu.SecSpec.1824	Info	Measure ID: M00060	--
Eu.SecSpec.1825	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• SCS</li></ul>	--
Eu.SecSpec.1828	Info	Threats: <ul style="list-style-type: none"><li>• T 040 Denial of Service</li><li>• T 027 Lack of Resources</li></ul>	--
Eu.SecSpec.1830	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SR 2.7</li><li>• SR 7.1, SR 7.1 RE 1, SR 7.1 RE 2</li></ul>	--
Eu.SecSpec.2997	Head	<b>2.8.7.2 SCS</b>	
Eu.SecSpec.1787	Req	The SCS shall prioritize SCS management traffic.	All
Eu.SecSpec.1788	Req	The SCS shall provide management functionality even under circumstances caused by attacks.	All
Eu.SecSpec.3125	Head	<b>2.8.7.3 MDM, SSP, EIL</b>	
Eu.SecSpec.1834	Req	During Denial of Service (DoS) events, the component shall be able to manage high loads.	All
Eu.SecSpec.2999	Req	During Denial of Service (DoS) events, the component shall provide a degraded mode according to IEC 62443 SR 7.1, SR 7.1 RE 1 and SR 7.1 RE 2.	All
Eu.SecSpec.2807	Req	The IM shall define if a degraded mode shall exist.	IM
Eu.SecSpec.3000	Req	If a degraded mode is required, the IM shall define which component shall operate with minimal functionality.	IM
Eu.SecSpec.1836	Req	The component shall limit the number of concurrent sessions according to IEC 62443 SR 2.7.	All
Eu.SecSpec.1861	Head	<b>2.8.8 M00064: Limit resources of security functions</b>	
Eu.SecSpec.2780	Head	<b>2.8.8.1 General</b>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1863	Info	Measure ID: M00064	--
Eu.SecSpec.1864	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.1869	Info	Threats: <ul style="list-style-type: none"> <li>• T 040 Denial of Service</li> <li>• T 045 Data Loss</li> </ul>	--
Eu.SecSpec.1872	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 7.2</li> </ul>	--
Eu.SecSpec.1875	Req	The component shall limit use of system resources for security functions according to IEC 62443 SR 7.2.	All
Eu.SecSpec.1876	Head	<b>2.9 Organisational Security and Processes (OSP)</b>	
Eu.SecSpec.1877	Head	<b>2.9.1 M00003: Integrate security into processes</b>	
Eu.SecSpec.2741	Head	<b>2.9.1.1 General</b>	
Eu.SecSpec.1879	Info	Measure ID: M00003	--
Eu.SecSpec.1880	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.1886	Info	Threats: <ul style="list-style-type: none"> <li>• T 018 Bad Planning or Lack of Adaption</li> </ul>	--
Eu.SecSpec.1888	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• SR 4.2</li> </ul>	--
Eu.SecSpec.3126	Info	In this measure the term patch addresses security patches according to IEC 62443.	--
Eu.SecSpec.1892	Head	<b>2.9.1.2 EIL, MDM, SSP, EfeS, and ILS-Adapter</b>	
Eu.SecSpec.1893	Req	The IM shall align procedural requirements from security operation procedures with railway operation procedures.	IM
Eu.SecSpec.3001	Req	The IM shall align procedural requirements from security maintenance procedures with railway maintenance procedures.	IM
Eu.SecSpec.1955	Head	<b>2.9.1.3 Patch-Process</b>	
Eu.SecSpec.3002	Info	Patch management processes are part of the operational phase of the lifecycle.	--
Eu.SecSpec.3003	Req	The IM shall define legally binding responsibilities for parties involved in the patch process of the component.	IM
Eu.SecSpec.3004	Req	The IM shall define legally binding duties for parties involved in the patch process of the component.	IM
Eu.SecSpec.3005	Req	The IM shall define procedures for the patch process of the component.	IM
Eu.SecSpec.3006	Info	The following patch process example may be implemented by the IM.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.1957	Info	To check if a patch can be applied in an EULYNX system, the patch process (Figure 2) checks organisational, regulatory and technical preconditions. After a patch (a changed software version) becomes available, the characteristics of the patch and its changes are to be determined. If the patch introduces new functionalities, it can be checked for conformity with the product specifications. In the case that the conformity cannot be proven, the patch cannot be applied. Then it's necessary to carry out a vulnerability assessment which results in either a mitigating measure or the decision to accept the risk. Assuming that the patch does not contain new functionalities, or the novel functionalities are still compliant the process can continue and result in two checks:	--
Eu.SecSpec.1958	Info	<ul style="list-style-type: none"> <li>Check for security certificate violation:</li> </ul>	--
Eu.SecSpec.1959	Info	<ul style="list-style-type: none"> <li>To check for the possible conformity with the existing security certificate of the product, the security certificate violation process (Figure 4) can be started. It checks for further characteristics of the patch. Updates to basic system components like the operating system and drivers do not negatively affect the certification.</li> </ul>	--
Eu.SecSpec.1960	Info	<ul style="list-style-type: none"> <li>Assuming that configuration changes are reduced to parameters having no effect on the security of the product, certification is not affected as a result.</li> </ul>	--
Eu.SecSpec.1961	Info	<ul style="list-style-type: none"> <li>If the patch can be categorized as a library update only, it does not violate the certificate if the changes do not affect the API or the functionalities of the library (minor update).</li> </ul>	--
Eu.SecSpec.1962	Info	<ul style="list-style-type: none"> <li>A general software update is not further categorised in this example and is thus automatically considered to negatively affect the security certification.</li> </ul>	--
Eu.SecSpec.1963	Info	<ul style="list-style-type: none"> <li>Check for violation of other approvals:</li> </ul>	--
Eu.SecSpec.1964	Info	<ul style="list-style-type: none"> <li>The IM checks that the patch is compliant to other approvals. As the approval highly depends on nation specific standards, the process is to be defined by the IM. The process has to include safety approvals.</li> </ul>	--
Eu.SecSpec.1965	Info	If the patch affects the security certification or other approvals, it has to be checked whether the patch can be used for interim operation without full certification or approval. In the case that both checks result in either no affection on the certificate/approvals or a possible operation without the certificates/approvals, the necessary test scope must be defined. If that is not possible the vulnerability assessment process has to be started.	--
Eu.SecSpec.3007	Info	After the tests have been performed based on the defined test scope, the results have to be analysed. An unsuccessful test could result in a release of the patch if the malfunction is acceptable or a short-term solution for the detected problems is available. Otherwise, the patch cannot be used, and a vulnerability assessment has to be carried out.	--
Eu.SecSpec.1966	Info	The patch is to be tested according to the defined tests scope. The test results have to be assessed. Failed test cases may be further analysed. Acceptance of failed test cases may lead to release the patch for rollout for a short-usage time or in combination with additional measures/workarounds. If patch rollout is not justifiable, the vulnerability management and assessment process has to be started.	--
Eu.SecSpec.1967	Info	If the patch has qualified for rollout, the rollout may be done as soon as possible.	--
Eu.SecSpec.3008	Info	To decrease the negative effects of the patch and possible downtimes, redundant systems can be used. For this purpose, an additional redundant system must be put in operation. While one of the systems (System A) is active, the other system (System B) can be updated, and the patch can be installed. After the successful completion of the patch and a possible additional test, the passive system (System B) can take over the operation and become the active system. After the correct operation of the active system (System B), the now passive system (System A) can be updated as well and both systems can return to standard operation. The design decision for redundancy to support patch-rollout may to be by each IM and may lead to location dependant decisions.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2721	Info	<div>Figure 2: Patch and Test Process (Part 1)</div> <pre>graph TD; Start([Start]) --&gt; Patch[Changed Software (Patch)]; Patch --&gt; Decision{Patch contains new functionality?}; Decision -- no --&gt; A{{A}}; Decision -- yes --&gt; Check[Check patch for conformity with specifications]; Check --&gt; B{{B}}</pre>	--



ID	Type	Requirement	Valid for
Eu.SecSpec.2740	Info	<p>Figure 2: Patch and Test Process (Part 2)</p> <pre> graph TD     A{{A}} --&gt; C1[Check for security certificate violation]     B{{B}} --&gt; C2{complies}     C2 -- no --&gt; V[<b>Vulnerability assessment process: mitigating measure or risk acceptance</b>]     C2 -- yes --&gt; C1     C1 --&gt; D1{Does the patch affect the security certification?}     D1 -- yes --&gt; A1[Assess whether interim operation is possible without full certification or approval.]     A1 --&gt; D2{Operation possible without a certificate?}     D2 -- yes --&gt; E2{E=2}     E2 -- yes --&gt; C{{C}}     E2 -- no --&gt; D{{D}}     D1 -- no --&gt; D     C1 --&gt; C3[Check for violation of other approval?]     C3 --&gt; D3{Does Patch affect other relevant approvals (e.g. non-retroactivity)?}     D3 -- yes --&gt; A2[Assess whether interim operation is possible without full certification or approval.]     A2 --&gt; D4{Operation possible without approval?}     D4 -- yes --&gt; D     D4 -- no --&gt; E{{E}}     D3 -- no --&gt; D     </pre> <p>Needs to be defined by the IM due to nation specific approval processes for safety</p>	--
Eu.SecSpec.3143	Info	Note: E=2 means that both inputs must be "yes".	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2722	Info	<p>Figure 2: Patch and Test Process (Part 3)</p> <pre> graph TD     C{{C}} --&gt; A[Determination of necessary test scope]     A --&gt; B{Test successful?}     B -- yes --&gt; F[Release]     B -- no --&gt; D{Malfunction acceptable or short-term solution possible?}     D -- yes --&gt; F     D -- no --&gt; G[Vulnerability assessment process: mitigating measure or risk acceptance]     G -- D --&gt; End([End])     G -- E --&gt; End     F --&gt; H[Apply patch]     H --&gt; End   </pre>	--
Eu.SecSpec.1971	Info	Figure 4 shows an example for a certificate violation assessment process.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2723	Info	<p>Figure 4: Security Certificate Violation Process</p> <pre> graph TD     Start([Start]) --&gt; S1{System update? (OS, Drivers, etc.)}     S1 --&gt; S2{Configuration update?}     S2 --&gt; S3{Library update?}     S3 -- yes --&gt; S4{Minor or major library update?}     S3 -- no --&gt; S5{Software update?}     S5 -- yes --&gt; S6{Major library update or software update?}     S4 -- major --&gt; S6     S4 -- minor --&gt; S2     S6 -- yes --&gt; V1([Does violate certification])     S6 -- no --&gt; V2([Does not violate certification]) </pre>	--
Eu.SecSpec.1978	Head	<b>2.9.1.4 Vulnerability Management</b>	
Eu.SecSpec.3009	Info	Vulnerability management processes are part of the operational phase of the lifecycle.	--
Eu.SecSpec.3010	Req	The IM shall define legally binding responsibilities for parties involved in the vulnerability management process of the component.	IM
Eu.SecSpec.3011	Req	The IM shall define legally binding duties for parties involved in the vulnerability management process of the component.	IM
Eu.SecSpec.3012	Req	The IM shall define procedures for the vulnerability management process of the component.	IM
Eu.SecSpec.3013	Req	The IM shall define procedures to evaluate the severity level of a vulnerability.	IM
Eu.SecSpec.3014	Req	The IM shall define procedures to evaluate the railway specific impact for every vulnerability.	IM
Eu.SecSpec.3015	Req	The IM shall require the suppliers to a coordinated vulnerability disclosure procedure following ISO 29147.	IM
Eu.SecSpec.3016	Req	The supplier shall provide information about a new vulnerability affecting the system to the IM within 24 hours after the vulnerability has been identified and assessed by the supplier.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.3017	Req	The supplier shall provide information on countermeasures regarding a vulnerability affecting the system to the IM within 24 hours after the countermeasure has been identified and assessed by the supplier.	All
Eu.SecSpec.3018	Info	Countermeasures include updates or software patches.	--
Eu.SecSpec.3019	Req	The IM shall operate a vulnerability management database.	IM
Eu.SecSpec.3020	Req	The vulnerability management database shall be linked to the configuration management data base.	IM
Eu.SecSpec.3021	Info	The following vulnerability management process example may be implemented by the IM.	--
Eu.SecSpec.3022	Info	In the vulnerability management process the patch process mentioned above is automatically triggered. During the analysis of the vulnerability (Figure 5) affected systems are identified and the impact on the system is determined. The analysis of immediate measures is described in Figure 6.	--
Eu.SecSpec.1980	Info	As soon as a vulnerability of a system is discovered the vulnerability management process (Figure 5) is started. As a precondition for starting the process, it is assumed that the discovered vulnerability was verified to exist and being valid.	--
Eu.SecSpec.1981	Info	At first, affected systems have to be identified. If an affected system could be identified, the vulnerability assessment has to be carried out. Thus the impact of the vulnerability in the specific context is analysed. If no risk exists, the vulnerability does not directly need to be addressed and can be handled in the regular patch cycle. Otherwise, the impact on the surrounding system needs to be analysed per relevant system. The findings documents contain descriptions of the impact per component or subsystem. This analysis has to be repeated regularly if no current impact can be identified. The immediate measures process (Figure 6) is performed otherwise.	--
Eu.SecSpec.1982	Info	The immediate measures process evaluates every possible solution which can be implemented timely. First solution could be an emergency patch. If the patch is available and can be used immediately, it can directly be implemented. Either it can be used as a long-term solution and the patch and test process is triggered or the process will close with the direct implementation and documentation of the patch. Possible compensating measures have to be evaluated if no patch can be used (immediately). The evaluation may consider threat probability and the effort to apply the possible measures. Three different kinds of measures are possible and all of them have to be evaluated at first:	--
Eu.SecSpec.1983	Info	<ul style="list-style-type: none"> <li>• Procedural measures e.g. changes in the maintenance lifecycle of the system, additional training for the technical personnel</li> </ul>	--
Eu.SecSpec.1984	Info	<ul style="list-style-type: none"> <li>• Technical measures e.g. configuration changes, or replacement</li> </ul>	--
Eu.SecSpec.1985	Info	<ul style="list-style-type: none"> <li>• Mechanical measures e.g. adding additional physical protection</li> </ul>	--
Eu.SecSpec.1986	Info	The preferred measure has to be chosen from the derived possible solutions. After the measure has been applied, it has to be documented and the process ends.	--
Eu.SecSpec.1987	Info	Based on the results of the immediate measures process the vulnerability management process (Figure 5) can continue. If the previous process (Figure 6) could not provide an immediate patch or measure, a decision has to be made on risk acceptance. Either a risk acceptance or a risk avoidance strategy needs to be chosen. Both options need to be documented. Furthermore, both options result in a repetitive subprocess which continuously checks for a permanent solution. This subprocess is also triggered if an immediate patch is available but can not be used as a permanent solution. The subprocess only stops if a permanent solution is implemented in the patch and test process. All decisions and the evaluation criteria have to be documented.	--
Eu.SecSpec.1997	Info	The operator may update redundant systems in a step by step process to ensure roll-back possibility.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2724	Info	<p>Figure 5: Vulnerability Management Process (part 1)</p> <pre> graph TD     Start([Vulnerability has been discovered]) --&gt; Identify[Identify affected systems]     Identify --- AR[Asset-Repository]     Identify --&gt; Affected{System affected?}     Affected -- no --&gt; Patch[Handling in the regular patch cycle]     Affected -- yes --&gt; Assess[Vulnerability assessment&lt;br/&gt;(Impact of the vulnerability in the specific context)]     Assess --- SD1[Systemdesign]     Assess --&gt; Risk{Risk existing?}     Risk -- no --&gt; Patch     Risk -- yes --&gt; Impact[Impact analysis on the surrounding system per relevant system]     Impact --- SD2[Systemdesign]     Impact --&gt; ImpactExist{Impact existing?}     ImpactExist -- no --&gt; Repeat[Repeat impact analysis regularly]     ImpactExist -- yes --&gt; A{{A}}     Patch --&gt; B{{B}}     Repeat --&gt; B   </pre>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2739	Info	<p>Figure 5: Vulnerability Management Process (part 2)</p> <pre> graph TD     A[A] --&gt; IM[Immediate measures]     IM --&gt; D1{Can immediate patch or measure be applied?}     D1 -- yes --&gt; D2{Can the patch be used as long term solution?}     D1 -- no --&gt; DRA[Documentation of risk acceptance]     D2 -- yes --&gt; B[B]     D2 -- no --&gt; DRA     DRA --&gt; C[Check for permanent solution]     C --&gt; D3{Permanent solution available?}     D3 -- yes --&gt; PTP[Patch and test process]     D3 -- no --&gt; C     PTP --&gt; DEC[Documentation of evaluation criteria]     DEC --&gt; VC([Vulnerability covered])     ART[Assessment result Tasks]   </pre>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2725	Info	<p>Figure 6: Immediate Measures Process</p> <pre> graph TD     Start([Start]) --&gt; D1{Patch available immediately?}     D1 -- yes --&gt; D2{Determine if patch can be used as immediate measure}     D2 -- yes --&gt; D3{Patch can be used immediately?}     D3 -- yes --&gt; D4{Patch can be used as long term solution?}     D4 -- yes --&gt; PTP[Patch and test process]     D4 -- no --&gt; D5{Implementation and documentation of (emergency) patch}     D1 -- no --&gt; E1[Evaluate of possible compensating measures regarding threat propability and effort to apply the measure.]     D3 -- no --&gt; E1     D2 -- no --&gt; E1     D3 -- no --&gt; E1     E1 --&gt; D6{Procedural measure possible and preferred?}     D6 -- yes --&gt; A1[Apply procedural measure]     D6 -- no --&gt; D7{Technical measure possible and preferred?}     D7 -- yes --&gt; A2[Apply technical measure]     D7 -- no --&gt; D8{Mechanical measure possible and preferred?}     D8 -- yes --&gt; A3[Apply mechanical measure]     D8 -- no --&gt; D9[Documentation of compensating measure]     A1 --&gt; D9     A2 --&gt; D9     A3 --&gt; D9     PTP --&gt; End([End])     D5 --&gt; End     D9 --&gt; End   </pre>	--
Eu.SecSpec.1999	Info	The IM may define a method for evaluating vulnerabilities. The CVSS (Common Vulnerability Scoring System) is the most common method. It allows to quantify the severity and risk of a vulnerability to an information asset in a computing environment.	--
Eu.SecSpec.2001	Info	The vulnerability may be assessed based on the railway-specific impact. Therefore, the factor of CVSS is taken and the railway specific factor is attached (Figure 7). The application is explained afterwards.	--

ID	Type	Requirement	Valid for																												
Eu.SecSpec.2726	Info	<div>Figure 7: Railway specific vulnerability assessment</div> <div><pre>graph TD; A([vulnerability assessment]) --&gt; B[Initial assessment through ,standard' process]; B --&gt; C[Assessment potential impact]; C --&gt; D[Assessment of affected systems]; D --&gt; E([Vulnerability assessed]);</pre><p>The flowchart illustrates the railway specific vulnerability assessment process. It begins with an oval labeled 'vulnerability assessment', which leads to a rectangular box 'Initial assessment through ,standard' process'. To the left of this box is a rounded rectangle labeled ',standard' process (e.g. CVSS)'. The flow continues to a box 'Assessment potential impact', then to 'Assessment of affected systems'. These two boxes are enclosed within a larger rectangle labeled 'Consideration Railway specific factors'. Finally, the process ends at an oval labeled 'Vulnerability assessed'.</p></div>	--																												
Eu.SecSpec.2007	Info	Figure 8 shows an impact matrix for the railway domain.	--																												
Eu.SecSpec.2008	Info	<div>Figure 8: Assessment of potential impact</div> <table><tr><td rowspan="3">Potential Impact</td><td>Directly</td><td>serious</td><td>serious</td><td>critical</td><td>critical</td></tr><tr><td>Connected</td><td>moderate</td><td>serious</td><td>serious</td><td>critical</td></tr><tr><td>Indirectly</td><td>moderate</td><td>moderate</td><td>serious</td><td>serious</td></tr><tr><td></td><td></td><td>Low</td><td>Middle</td><td>High</td><td>Very high</td></tr><tr><td></td><td></td><td colspan="4">Initial evaluation of vulnerability</td></tr></table>	Potential Impact	Directly	serious	serious	critical	critical	Connected	moderate	serious	serious	critical	Indirectly	moderate	moderate	serious	serious			Low	Middle	High	Very high			Initial evaluation of vulnerability				--
Potential Impact	Directly	serious		serious	critical	critical																									
	Connected	moderate		serious	serious	critical																									
	Indirectly	moderate	moderate	serious	serious																										
		Low	Middle	High	Very high																										
		Initial evaluation of vulnerability																													
Eu.SecSpec.2009	Info	Table 4 shows the definition of the potential impact in the railway domain.	--																												
Eu.SecSpec.2010	Info	Table 4 Definition of potential impact	--																												



ID	Type	Requirement	Valid for																							
Eu.SecSpec.2010		<table><tr><th>Parameter</th><th>Description</th></tr><tr><td>Directly</td><td>The vulnerability concerns a system that directly bears safety responsibility (safety relevant EN 50126 or functional safety in general) for railway operations and whose manipulation must be expected to cause fatalities.</td></tr><tr><td>Connected</td><td>The vulnerability concerns a system,  - that is a safety barrier (safety relevant EN 50126 or functional safety in general) in a system with direct safety responsibility, the manipulation of which is not expected to result in fatalities (e.g. access mechanisms)  - which has indirect safety responsibility (safety relevant EN 50126) for railway operations and whose manipulation requires other independent safety barriers to be overcome before an accident occurs.</td></tr><tr><td>Indirectly</td><td>The vulnerability concerns a system without safety responsibility (safety relevant EN 50126 or functional safety in general) but brings a share in the safety of the operational business.</td></tr></table>	Parameter	Description	Directly	The vulnerability concerns a system that directly bears safety responsibility (safety relevant EN 50126 or functional safety in general) for railway operations and whose manipulation must be expected to cause fatalities.	Connected	The vulnerability concerns a system,  - that is a safety barrier (safety relevant EN 50126 or functional safety in general) in a system with direct safety responsibility, the manipulation of which is not expected to result in fatalities (e.g. access mechanisms)  - which has indirect safety responsibility (safety relevant EN 50126) for railway operations and whose manipulation requires other independent safety barriers to be overcome before an accident occurs.	Indirectly	The vulnerability concerns a system without safety responsibility (safety relevant EN 50126 or functional safety in general) but brings a share in the safety of the operational business.																
Parameter	Description																									
Directly	The vulnerability concerns a system that directly bears safety responsibility (safety relevant EN 50126 or functional safety in general) for railway operations and whose manipulation must be expected to cause fatalities.																									
Connected	The vulnerability concerns a system,  - that is a safety barrier (safety relevant EN 50126 or functional safety in general) in a system with direct safety responsibility, the manipulation of which is not expected to result in fatalities (e.g. access mechanisms)  - which has indirect safety responsibility (safety relevant EN 50126) for railway operations and whose manipulation requires other independent safety barriers to be overcome before an accident occurs.																									
Indirectly	The vulnerability concerns a system without safety responsibility (safety relevant EN 50126 or functional safety in general) but brings a share in the safety of the operational business.																									
Eu.SecSpec.2011	Info	The intermediate result from Figure 8 (critical, serious, moderate) is used as input in Figure 9 to consider the affected systems.	--																							
Eu.SecSpec.2013	Info	Figure 9 shows a need of action matrix.	--																							
Eu.SecSpec.2014	Info	Figure 9: Need of action matrix <table><tr><td rowspan="3">Dispersion in railway system</td><td>All</td><td>mid term</td><td>short term</td><td>immediate</td></tr><tr><td>Multiple</td><td>long term</td><td>mid term</td><td>short term</td></tr><tr><td>Single</td><td>none</td><td>long term</td><td>mid term</td></tr><tr><td></td><td></td><td>moderate</td><td>serious</td><td>critical</td></tr><tr><td></td><td></td><td colspan="3">Category (from impact table)</td></tr></table>	Dispersion in railway system	All	mid term	short term	immediate	Multiple	long term	mid term	short term	Single	none	long term	mid term			moderate	serious	critical			Category (from impact table)			--
Dispersion in railway system	All	mid term		short term	immediate																					
	Multiple	long term		mid term	short term																					
	Single	none	long term	mid term																						
		moderate	serious	critical																						
		Category (from impact table)																								
Eu.SecSpec.2015	Info	The evaluation of the propagation in the railway system uses the following proposed scale, which was supplemented by the aspect of the scalability of the exploitation of the vulnerability. The definition is shown in Table 5.	--																							
Eu.SecSpec.2018	Info	Table 5: Scale of spreading	--																							

ID	Type	Requirement		Valid for
Eu.SecSpec.2018		Parameter	Description	
		Single	The vulnerability affects a system with a regional reference or a geographically limited area or a single system (e.g. signal, switch) in the overall system. Exploitation of the vulnerability requires access to each individual system or access to each individual system (scalability).	
		Multiple	The vulnerability affects a system that is used several times in the same form in the entire railway system or a facility (e.g. axle counting systems of one type, all signals of an interlocking). The vulnerability can be exploited simultaneously on the affected systems (scalability), i.e. the effects are no longer regional or limited to a single installation.	
		All	The vulnerability affects the railway system as a whole or is on a base system that is used by a number of other systems. The vulnerability can be exploited in such a way that it affects the entire railway system (scalability).	
Eu.SecSpec.2021	Info	Table 6 describes the need for action in terms of time based on Figure 9.		--
Eu.SecSpec.2024	Info	Table 6: Time scale for action		--
		Speed of action	definition	
		Immediate	Immediate action must be taken within 48 hours.	
		Short term	Action must be taken within one week.	
		Mid term	Action must be taken within one month.	
		Long term	Action must be taken within three months.	
		None	It is sufficient to consider the vulnerability within the normal patch cycle.	
Eu.SecSpec.2025	Head	2.9.1.5 First operation and re-commissioning		
Eu.SecSpec.2029	Req	The IM shall define first-operation and re-commission procedures ensuring system integrity checks of the component.		IM
Eu.SecSpec.3023	Req	The IM shall define first-operation and re-commission procedures ensuring that the validity of certificate signing requests is assured.		IM
Eu.SecSpec.3024	Info	The certificate signing procedure is part of the initial identity provisioning, establishing an initial trust.		--
Eu.SecSpec.3025	Req	The IM shall define first-operation and re-commission procedures ensuring start of security monitoring of the component.		IM
Eu.SecSpec.3026	Head	2.9.1.6 Decommissioning		
Eu.SecSpec.3027	Info	The decommissioning process is triggered if the component is put temporarily or permanently out of service.		--
Eu.SecSpec.3028	Req	The IM shall revoke certificates of the component during decommissioning.		IM
Eu.SecSpec.3029	Req	The IM shall revoke the NAC access of the component during decommissioning.		IM

ID	Type	Requirement	Valid for
Eu.SecSpec.3030	Req	The IM shall remove access rights of the component during decommissioning.	IM
Eu.SecSpec.3031	Req	The IM shall change the status of the component in the asset management to decommissioned.	IM
Eu.SecSpec.3032	Req	The IM shall remove sensitive data stored on the component in a permanent and secure way during decommissioning.	IM
Eu.SecSpec.3033	Req	The IM shall define decommission procedures ensuring stopping the security monitoring of the component.	IM
Eu.SecSpec.3034	Req	The IM shall document the decommissioning process.	IM
Eu.SecSpec.2036	Head	<b>2.9.1.7 Documentation</b>	
Eu.SecSpec.2038	Req	The IM shall ensure that the system is documented.	IM
Eu.SecSpec.2041	Req	The IM shall ensure that the system documentation includes the system design.	IM
Eu.SecSpec.2042	Req	The IM shall ensure that the system documentation includes the network architecture.	IM
Eu.SecSpec.2043	Req	The IM shall ensure that the system documentation includes the requirement specifications.	IM
Eu.SecSpec.2044	Req	The IM shall ensure that the system documentation includes the component specification.	IM
Eu.SecSpec.2045	Req	The IM shall ensure that the system documentation includes the interface specification of EULYNX interfaces.	IM
Eu.SecSpec.3036	Req	The IM shall ensure that the system documentation includes the interface specification of supplier-specific interfaces.	IM
Eu.SecSpec.2046	Req	The IM shall ensure that the system documentation includes the dependencies.	IM
Eu.SecSpec.2047	Req	The IM shall ensure that the system documentation includes the SRACs.	IM
Eu.SecSpec.2048	Req	The IM shall ensure that the system documentation includes the SecRACs.	IM
Eu.SecSpec.2049	Req	The IM shall ensure that the system documentation includes the process and guideline documentation.	IM
Eu.SecSpec.3037	Req	The IM shall ensure that the system documentation includes the default settings.	IM
Eu.SecSpec.2050	Req	The IM shall ensure that the system documentation includes the maintenance documentation.	IM
Eu.SecSpec.2051	Req	The IM shall ensure that the system documentation includes the service level agreement, QoS definitions.	IM
Eu.SecSpec.2052	Req	The IM shall ensure that the system documentation includes the service contracts.	IM
Eu.SecSpec.2053	Req	The IM shall ensure that the system documentation includes the results from TIC (tester in charge).	IM
Eu.SecSpec.2054	Req	The IM shall ensure that the system documentation includes the site acceptance test.	IM
Eu.SecSpec.2055	Req	The IM shall ensure that the system documentation includes the interoperability test.	IM
Eu.SecSpec.3038	Req	The IM shall ensure that the system documentation includes system and component quality, safety and security certification.	IM
Eu.SecSpec.2057	Req	The IM shall operate a configuration management data base.	IM
Eu.SecSpec.3039	Req	The IM shall operate an asset management system.	IM
Eu.SecSpec.2059	Req	The asset management shall include the software version.	IM
Eu.SecSpec.2060	Req	The asset management shall include the hardware version.	IM
Eu.SecSpec.2061	Req	The asset management shall include the firmware version.	IM
Eu.SecSpec.2062	Req	The asset management shall include the parameter configuration version.	IM
Eu.SecSpec.2063	Req	The asset management shall include the asset relation and hierarchy.	IM

ID	Type	Requirement	Valid for
Eu.SecSpec.2064	Req	The asset management shall include the used security measures/functionalities.	IM
Eu.SecSpec.2065	Req	The asset management shall include the life cycle information.	IM
Eu.SecSpec.2066	Req	The asset management shall include the set-up date.	IM
Eu.SecSpec.2067	Req	The asset management shall include the date of delivery.	IM
Eu.SecSpec.2068	Req	The asset management shall include the date of foreseen end of life.	IM
Eu.SecSpec.2069	Req	The asset management shall include the date of foreseen end of support.	IM
Eu.SecSpec.2070	Req	The asset management shall include the date of foreseen decommissioning.	IM
Eu.SecSpec.3040	Req	The configuration management data base shall include the software version.	IM
Eu.SecSpec.3041	Req	The configuration management data base shall include the hardware version.	IM
Eu.SecSpec.3042	Req	The configuration management data base shall include the firmware version.	IM
Eu.SecSpec.3043	Req	The configuration management data base shall include the parameter configuration.	IM
Eu.SecSpec.3044	Req	The configuration management data base shall include the asset relation and hierarchy.	IM
Eu.SecSpec.3045	Req	The configuration management data base shall include the set-up date.	IM
Eu.SecSpec.2081	Req	The IM shall operate a change management tool.	IM
Eu.SecSpec.3046	Req	The change management tool shall track changes to systems and components.	IM
Eu.SecSpec.3047	Head	<b>2.9.1.8 Monitoring</b>	
Eu.SecSpec.3048	Req	The IM shall define procedures to check the system integrity after an interruption of the system's security monitoring.	IM
Eu.SecSpec.3049	Info	The integration of system integrity aspect into monitoring as an illustrative proposal:	--
Eu.SecSpec.3050	Info	The seals and components may be checked for manipulation after loss of continuous monitoring (SIEM) due to power interruption or loss of network connection.	--
Eu.SecSpec.3051	Info	The check for manipulation may be performed after interruption of a specified time, e.g. 3 hours.	--
Eu.SecSpec.2091	Head	<b>2.9.2 M00014: Supply chain security</b>	
Eu.SecSpec.2781	Head	<b>2.9.2.1 General</b>	
Eu.SecSpec.2093	Info	Measure ID: M00014	--
Eu.SecSpec.2094	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• EfeS</li><li>• SCS</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.2100	Info	Threats: <ul style="list-style-type: none"><li>• T 011 Failure or Disruption of Service Providers</li></ul>	--
Eu.SecSpec.2102	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• None</li></ul>	--
Eu.SecSpec.2105	Req	The IM shall define rules and procedures to implement supply chain security.	IM
Eu.SecSpec.2114	Head	<b>2.9.2.2 Supplier Management</b>	

ID	Type	Requirement	Valid for
Eu.SecSpec.3052	Req	The IM shall establish an escrow agreement to protect from bankruptcy or market exit of the supplier	IM
Eu.SecSpec.3053	Req	The supplier shall store the source code of the system at the escrow agent.	All
Eu.SecSpec.3054	Req	The supplier shall store the internal documentation of the system at the escrow agent.	All
Eu.SecSpec.2146	Head	<b>2.9.2.3 Production</b>	
Eu.SecSpec.2148	Req	The supplier shall establish and maintain ISO 27001 certification for the production organisation.	All
Eu.SecSpec.3055	Req	The supplier shall establish and maintain ISO 27001 certification for the software development organisation.	All
Eu.SecSpec.3056	Req	The supplier shall seal the hardware to indicate manipulation.	All
Eu.SecSpec.3057	Req	The supplier shall seal the hardware at least at component level.	All
Eu.SecSpec.3058	Req	The seals shall visibly indicate manipulation.	All
Eu.SecSpec.3131	Req	The component documentation shall include information to differentiate intact and broken seals.	All
Eu.SecSpec.3059	Req	The seals shall be tamper proof.	All
Eu.SecSpec.2157	Head	<b>2.9.2.4 Transport</b>	
Eu.SecSpec.2159	Req	The supplier shall seal the transport container to indicate manipulation.	All
Eu.SecSpec.3060	Req	The supplier shall track transport steps incl. means of transport and storage time	All
Eu.SecSpec.3061	Req	The IM shall check the seal of the transport container on arrival.	IM
Eu.SecSpec.2160	Head	<b>2.9.2.5 Commissioning process</b>	
Eu.SecSpec.2162	Info	To avoid manipulation in between delivery by the supplier and start of operation (powered and monitored) suitable measures might be defined by the IM.	--
Eu.SecSpec.2164	Req	The IM shall store the components in a surveyed storage with limited access with identity and access management using personal identification	IM
Eu.SecSpec.3062	Req	The IM shall check the seal of the component prior to commissioning.	IM
Eu.SecSpec.2186	Req	If a component is set into operation for the first time, the component shall load software and configuration from the central management server.	All
Eu.SecSpec.3063	Req	If a component is replaced, the component shall load software and configuration from the central management server.	All
Eu.SecSpec.2189	Head	<b>2.9.3 M00016: Procurement strategy</b>	
Eu.SecSpec.2782	Head	<b>2.9.3.1 General</b>	
Eu.SecSpec.2191	Info	Measure ID: M00016	--
Eu.SecSpec.2192	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.2198	Info	Threats: <ul style="list-style-type: none"> <li>• T 011 Failure or Disruption of Service Providers</li> <li>• T 020 Information or Products from an Unreliable Source</li> <li>• T 028 Software Vulnerabilities or Errors</li> </ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2202	Info	Reference to IEC 62443: • None	--
Eu.SecSpec.2205	Req	The IM shall implement a multi-vendor strategy.	IM
Eu.SecSpec.3064	Req	The IM shall implement a strategy for purchasing technically dissimilar components.	IM
Eu.SecSpec.3065	Req	The IM shall establish processes to reduce the dependency on suppliers of subcomponents.	IM
Eu.SecSpec.2206	Info	This includes production, supply chains for productions, delivery, stock logistic, technical concepts/architectures, technical components, and software code.	--
Eu.SecSpec.3066	Info	Requiring standardized interfaces or technical parameters enhance inter-changeability of components. Following EULYNX is one concise set of interfaces and parameters designed for that purpose.	--
Eu.SecSpec.2207	Head	<b>2.9.4 M00017: Management of service providers</b>	
Eu.SecSpec.2783	Head	<b>2.9.4.1 General</b>	
Eu.SecSpec.2209	Info	Measure ID: M00017	--
Eu.SecSpec.2210	Info	Affected SuC: • SCS	--
Eu.SecSpec.2212	Info	Threats: • T 011 Failure or Disruption of Service Providers	--
Eu.SecSpec.2214	Info	Reference to IEC 62443: • None	--
Eu.SecSpec.3067	Info	This measure addresses the management of an SCS service provider. If other SuCs are operated by an service provider, similar requirements may be used by the IM.	--
Eu.SecSpec.2217	Req	The IM shall require their suppliers to implement the requirements for the management of service providers for their suppliers.	IM
Eu.SecSpec.3068	Req	The IM shall audit that suppliers implement the requirements for the management of service providers.	IM
Eu.SecSpec.3069	Info	A client of a service may be the IM or a supplier in the supply chain.	--
Eu.SecSpec.3070	Req	The client of a service shall include aspects of physical security in its service provider tender.	All
Eu.SecSpec.3071	Req	The client of a service shall include aspects of reliable service provisioning in its service provider tender.	All
Eu.SecSpec.3072	Req	The client of a service shall include aspects of availability of the provided service in its service provider tender.	All
Eu.SecSpec.3073	Req	The client of a service shall include aspects of black mail in its service provider tender.	All
Eu.SecSpec.3074	Req	The client of a service shall include aspects of political pressure in its service provider tender.	All
Eu.SecSpec.2218	Req	The service provider shall provide a security analysis covering the components required to provide the service to the client of the service every two years.	All
Eu.SecSpec.2219	Req	The service provider shall be certified according to ISO 27001 for the service provided.	All
Eu.SecSpec.2220	Req	The IM shall perform a resilience analysis for the service.	IM
Eu.SecSpec.3075	Req	The IM shall implement appropriate measures according to the resilience analysis for the service.	IM
Eu.SecSpec.2221	Info	The following measures could apply: • If the IM outsources the SCS, the IM may use a second service provider to reduce dependence of one partner. • If the IM outsources only the operation of the SCS, the IM may use an own network operation centre with own personnel to ensure minimal operational functionality.	--
Eu.SecSpec.2225	Head	<b>2.9.5 M00034: Detecting security vulnerabilities</b>	
Eu.SecSpec.2784	Head	<b>2.9.5.1 General</b>	
Eu.SecSpec.2227	Info	Measure ID: M00034	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2228	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• EfeS</li><li>• SCS</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.2234	Info	Threats: <ul style="list-style-type: none"><li>• T 018 Bad Planning or Lack of Adaption</li></ul>	--
Eu.SecSpec.2236	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• None</li></ul>	--
Eu.SecSpec.2249	Head	<b>2.9.5.2 Vulnerability scanning</b>	
Eu.SecSpec.2252	Req	The IM shall ensure that vulnerability scanning is performed for each component type and configuration setup at least every two years.	IM
Eu.SecSpec.2253	Req	The IM shall define a vulnerability scanning strategy.	IM
Eu.SecSpec.3076	Req	The IM shall define the scope for vulnerability scanning.	IM
Eu.SecSpec.3077	Req	The IM shall define a vulnerability scanning interval for each component type.	IM
Eu.SecSpec.2254	Req	The IM shall use a test instance of the system including each component type for vulnerability scanning.	IM
Eu.SecSpec.3078	Req	The test instance of the component under vulnerability scanning shall use the same software version as the production environment.	All
Eu.SecSpec.3079	Req	The test instance of the component under vulnerability scanning shall use the same hardware version as the production environment.	All
Eu.SecSpec.3080	Req	The test instance of the component under vulnerability scanning shall use a similar configuration as the production environment.	All
Eu.SecSpec.2260	Req	The test environment shall be isolated from the production environment.	All
Eu.SecSpec.3081	Req	The test instance of the component shall use a similar network setup as the production environment.	All
Eu.SecSpec.2262	Head	<b>2.9.5.3 Penetration-testing</b>	
Eu.SecSpec.2265	Req	The IM shall ensure that penetration testing is performed for each component type and configuration setup at least every two years.	IM
Eu.SecSpec.3082	Req	The IM shall ensure that penetration testing is performed for each component type and configuration setup for each software version.	IM
Eu.SecSpec.2266	Req	The IM shall define a penetration testing strategy.	IM
Eu.SecSpec.3083	Req	The IM shall define the scope for penetration testing.	IM
Eu.SecSpec.3084	Req	The IM shall define a penetration testing interval for each component type.	IM
Eu.SecSpec.3085	Req	The IM shall use a test instance of the system under penetration testing including each component type for penetration testing.	IM
Eu.SecSpec.3086	Req	The test instance of the component under penetration testing shall use the same software version as the production environment.	All
Eu.SecSpec.3087	Req	The test instance of the component under penetration testing shall use the same hardware version as the production environment.	All
Eu.SecSpec.3088	Req	The test instance of the component under penetration testing shall use a similar configuration as the production environment.	All
Eu.SecSpec.2272	Head	<b>2.9.6 M00035: Integration of security measures and components in railway operation procedures</b>	
Eu.SecSpec.2785	Head	<b>2.9.6.1 General</b>	
Eu.SecSpec.2274	Info	Measure ID: M00035	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2275	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• SCS</li> <li>• EfeS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.2281	Info	Threats: <ul style="list-style-type: none"> <li>• T 09 Failure or Disruption of Communication Networks</li> <li>• T 018 Bad Planning or Lack of Adaption</li> </ul>	--
Eu.SecSpec.2284	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2287	Info	Managing a security incident might require actions disturbing railway operation. In order to avoid unintentional railway service disruption, mitigating (e.g. isolating a network element) or investigative actions (e.g. re-routing of network traffic) by security operations should be coordinated between security operation and railway operation personnel. Railway operation may want to stop trains in stations to keep everything under control just in case something goes wrong.	--
Eu.SecSpec.3089	Req	The IM shall manage the interference between security procedures and railway operation procedures by implementing appropriate organisational structure, inter-process communication and responsibility extended with decision structures.	IM
Eu.SecSpec.2310	Head	<b>2.9.7 M00038: Security Awareness trainings for personnel</b>	
Eu.SecSpec.2787	Head	<b>2.9.7.1 General</b>	
Eu.SecSpec.2312	Info	Measure ID: M00038	--
Eu.SecSpec.2313	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.2317	Info	Threats: <ul style="list-style-type: none"> <li>• T 019 Disclosure of Sensitive Information</li> <li>• T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>• T 041 Sabotage</li> <li>• T 042 Social Engineering</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.2323	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2326	Req	The IM shall establish a security awareness training program for personnel which has access to sensitive information.	IM
Eu.SecSpec.3090	Info	Personnel which has access to sensitive information is e.g. working in SOC, CSIRT, NOC, network planning, energy planning, areas related to physical access control.	--
Eu.SecSpec.2328	Req	The IM shall ensure that internal and external personnel is trained regarding security awareness.	IM
Eu.SecSpec.2329	Req	The IM shall evaluate if the security awareness training fits to its needs.	IM
Eu.SecSpec.2331	Info	If the IM is not able or allowed to train external personnel directly, contractor-side equivalent trainings may be a requirement in the contracts and tenders. A sufficient proof of the quality of and the successful participation in awareness training may be requested from the external service provider.	--
Eu.SecSpec.2335	Head	<b>2.9.8 M00041: Dual control principle in software development</b>	
Eu.SecSpec.2788	Head	<b>2.9.8.1 General</b>	



ID	Type	Requirement	Valid for
Eu.SecSpec.2337	Info	Measure ID: M00041	--
Eu.SecSpec.2338	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li><li>• EfeS</li><li>• SCS</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.2344	Info	Threats: <ul style="list-style-type: none"><li>• T 021 Manipulation of Hardware or Software</li></ul>	--
Eu.SecSpec.2346	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SVV-5</li></ul>	--
Eu.SecSpec.2349	Req	The supplier shall implement the dual control principle in software development processes.	All
Eu.SecSpec.2350	Info	Software source code (static code analysis) may be checked by a person/group which was not part of the code writing process. This procedure may follow a formal approval process and may be documented.	--
Eu.SecSpec.2351	Head	<b>2.9.9 M00048: Testing procedures</b>	
Eu.SecSpec.2789	Head	<b>2.9.9.1 General</b>	
Eu.SecSpec.2353	Info	Measure ID: M00048	--
Eu.SecSpec.2354	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• EfeS</li><li>• MDM</li><li>• SSP</li><li>• SCS</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.2359	Info	Threats: <ul style="list-style-type: none"><li>• T 026 Malfunction of Devices or Systems</li></ul>	--
Eu.SecSpec.2361	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• SR 3.3, SR 3.3 RE 1</li><li>• CR 3.3</li></ul>	--
Eu.SecSpec.2365	Req	The IM shall test systems to reduce the risks of malfunctions in operation (functionality).	IM
Eu.SecSpec.3091	Req	The supplier shall test components to reduce the risks of malfunctions in operation (functionality).	All
Eu.SecSpec.2369	Head	<b>2.9.9.2 Functionality Testing</b>	
Eu.SecSpec.2371	Info	Functionality tests take place during development (following EN 50126 phases) and factory acceptance tests for components/products and site acceptance test after setup.	--
Eu.SecSpec.2372	Info	Some of these tests are done during the change/release management process of a larger system (phase 11).	--
Eu.SecSpec.2373	Head	<b>2.9.9.3 Security Related Component Testing</b>	
Eu.SecSpec.2385	Req	The supplier shall use an automated test tool for security functionality verification of components.	All
Eu.SecSpec.3092	Req	The IM shall use an automated test tool for security functionality verification of the system.	IM
Eu.SecSpec.2386	Req	The automated test tool shall include verification of security features of the component.	All
Eu.SecSpec.2387	Req	The automated test tool shall include verification of security parameter configuration of the component.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2392	Req	The automated test tool shall include verification of hardening of the component.	All
Eu.SecSpec.2394	Req	The automated test tool shall include verification of SSI functionality.	All
Eu.SecSpec.2397	Head	<b>2.9.9.4 Security Integration Testing</b>	
Eu.SecSpec.2398	Req	The IM shall define a test strategy for security related integration testing.	IM
Eu.SecSpec.3093	Req	The IM shall perform integration tests during CENELEC phase 9.	IM
Eu.SecSpec.3094	Req	The IM shall perform integration tests during CENELEC phase 11.	IM
Eu.SecSpec.3095	Head	<b>2.9.9.5 Security Testing Procedures</b>	
Eu.SecSpec.2399	Info	It is recommended to consider the following steps: 1. Component tests 2. Pre-integration tests 3. Integration tests 4. Field tests 5. Trial out with / without safety responsibility	--
Eu.SecSpec.2407	Info	Figure 11 shows an illustrative process which performs all necessary tests until the component can be deployed finally. If one of the following checks and tests fails the IM has to define the requirements of the change, which is afterwards requested from the vendor. After the vendor has delivered the changed component, the process may start again.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2728	Info	<p>Figure 11: Overall integration test process</p> <pre> graph TD     Start([Start]) --&gt; Analyse[Analyse specifications and preexisting tests of the vendor]     Analyse --&gt; Conform{Is the product conform to the requirements?}     Conform -- no --&gt; Define[Define change requirements]     Define --&gt; Request[Request changes from the vendor]     Request --&gt; Analyse     Conform -- yes --&gt; Functional[Perform functional tests]     Functional --&gt; Successful1{Successful?}     Successful1 -- no --&gt; Define     Successful1 -- yes --&gt; PreIntegration[Perform pre-integration tests]     PreIntegration --&gt; Successful2{Successful?}     Successful2 -- no --&gt; Define     Successful2 -- yes --&gt; SystemIntegration[Perform system integration tests]     SystemIntegration --&gt; Successful3{Successful?}     Successful3 -- no --&gt; Define     Successful3 -- yes --&gt; FieldTests[Perform field tests]     FieldTests --&gt; Successful4{Successful?}     Successful4 -- no --&gt; Define     Successful4 -- yes --&gt; OperationalTests[Perform operational tests]     OperationalTests --&gt; Successful5{Successful?}     Successful5 -- no --&gt; Define     Successful5 -- yes --&gt; End([End])   </pre>	--
Eu.SecSpec.2409	Info	The checks and test shown in Figure 11 are described as follows.	--
Eu.SecSpec.2410	Head	<b>2.9.9.5.1 Analyse specifications and pre-existing tests</b>	
Eu.SecSpec.2412	Info	The IM needs to check whether the specifications of the component meet the requirement for it. These requirements need to be defined prior to the start of this process. Furthermore, it is necessary to check for the conformity with regulatory requirements and industrial standards. The component requirements might include vendor-side tests. The test reports need to be checked and must plausibly represent the results.	--
Eu.SecSpec.2413	Head	<b>2.9.9.5.2 Functional test</b>	
Eu.SecSpec.2415	Info	In the functional tests the practical conformity of a function to the component description needs to be determined. Thus, it is possible to detect errors in the implementation or incompatibilities to the specification.	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2416	Head	<b>2.9.9.5.3 Pre-integration test</b>	
Eu.SecSpec.2418	Info	The pre-integration tests are carried out in a test environment. This environment needs to provide test data traffic and simulate all necessary interfaces and endpoints used by the component under test. Hence not only the application or component itself, but the communication in the network can be tested. Additionally, the management of the component needs to be addressed in the tests.	--
Eu.SecSpec.2419	Head	<b>2.9.9.5.4 System integration test</b>	
Eu.SecSpec.2421	Info	During the system integration tests the focus no longer lies on the functionality of the component in the network. Now the integration in the security environment is tested. Thus, the conformity to the security requirements needs to be addressed. Furthermore, the communication via the secure network is evaluated. Under the influence of the security functionalities test must be performed which check the management of the component, the correct communication, reactions to errors and analysis capabilities.	--
Eu.SecSpec.2422	Head	<b>2.9.9.5.5 Field test</b>	
Eu.SecSpec.2424	Info	After all necessary structural and technical measures have been implemented to prepare the implementation of the component, test can be performed which were not considered previously due to restrictions of the testing environment. Furthermore, tests have to be carried out again, which were only conducted to a limited technical level due to the laboratory environment (e.g., limited number of OCs in the testbed). All test which are required for the official approval of the system have to be done as well.	--
Eu.SecSpec.2425	Head	<b>2.9.9.5.6 Operational tests</b>	
Eu.SecSpec.2427	Info	During operational tests, the component is tested in the real operation of the overall system. That way the trouble-free operation of the component in railway operation can be asserted. Furthermore, the operation of the component can be tested regarding maintenance and monitoring.	--
Eu.SecSpec.2431	Head	<b>2.9.10 M00049: Human resources planning and training</b>	
Eu.SecSpec.2790	Head	<b>2.9.10.1 General</b>	--
Eu.SecSpec.2433	Info	Measure ID: M00049	--
Eu.SecSpec.2434	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.2440	Info	Threats: <ul style="list-style-type: none"> <li>• T 027 Lack of Resources</li> <li>• T 031 Incorrect Use or Administration of Devices and Systems</li> <li>• T 033 Absence of Personnel</li> <li>• T 035 Coercion, Extortion or Corruption</li> </ul>	--
Eu.SecSpec.2445	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2448	Req	The IM shall ensure the long-term human resource planning to provide sufficient staffing of qualified security personnel dedicated to operational technology	IM
Eu.SecSpec.3096	Info	The IM may include aspects of long-term availability of security personnel of the supplier in the tender and contracts.	--
Eu.SecSpec.2454	Head	<b>2.9.11 M00055: Privacy related information</b>	
Eu.SecSpec.2791	Head	<b>2.9.11.1 General</b>	
Eu.SecSpec.2456	Info	Measure ID: M00055	--
Eu.SecSpec.2457	Info	Affected SuC: <ul style="list-style-type: none"> <li>• SCS</li> <li>• MDM</li> <li>• SSP</li> </ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2459	Info	Threats: <ul style="list-style-type: none"><li>• T 029 Violation of Laws or Regulations</li><li>• T 037 Repudiation of Actions</li><li>• T 038 Abuse of Personal Data</li></ul>	--
Eu.SecSpec.2463	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• None</li></ul>	--
Eu.SecSpec.2466	Req	The system shall only save privacy related sensitive information in accordance with national regulation.	All
Eu.SecSpec.3097	Info	Works council agreements may apply in addition to national regulation.	--
Eu.SecSpec.2468	Info	Sensitive and privacy related information includes data which can be used to track the activities and performance of personnel.	--
Eu.SecSpec.2469	Head	<b>2.10 Physical Protection (PP)</b>	
Eu.SecSpec.2490	Head	<b>2.10.1 M00002: Physical protection</b>	
Eu.SecSpec.2793	Head	<b>2.10.1.1 General</b>	
Eu.SecSpec.2492	Info	Measure ID: M00002	--
Eu.SecSpec.2493	Info	Affected SuC: <ul style="list-style-type: none"><li>• EfeS</li><li>• SCS</li><li>• ILS-Adapter</li></ul>	--
Eu.SecSpec.2499	Info	Threats: <ul style="list-style-type: none"><li>• T 01 Fire</li><li>• T 024 Destruction of Devices or Storage Media</li><li>• T 034 Attack</li><li>• T 041 Sabotage</li><li>• T 044 Unauthorised Entry to Premises</li></ul>	--
Eu.SecSpec.2505	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>• None</li></ul>	--
Eu.SecSpec.3127	Req	The environment physically protecting the component shall be designed according to the local environmental threats.	All
Eu.SecSpec.3128	Req	The environment physically protecting the component shall be designed according to the local threats created by humans.	All
Eu.SecSpec.2513	Head	<b>2.10.2 M00005: Rules for locations with major importance</b>	
Eu.SecSpec.2794	Head	<b>2.10.2.1 General</b>	
Eu.SecSpec.2515	Info	Measure ID: M00005	--
Eu.SecSpec.2516	Info	Affected SuC: <ul style="list-style-type: none"><li>• EIL</li><li>• MDM</li><li>• SSP</li></ul>	--
Eu.SecSpec.2519	Info	Threats: <ul style="list-style-type: none"><li>• T 01 Fire</li><li>• T 03 Water</li><li>• T 05 Natural Disasters</li><li>• T 06 Environmental Disasters</li><li>• T 07 Major Events in the Environment</li><li>• T 012 Interfering Radiation</li><li>• T 024 Destruction of Devices or Storage Media</li><li>• T 034 Attack</li></ul>	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2528	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.2531	Req	The IM shall choose the location considering natural risks.	IM
Eu.SecSpec.3099	Info	Examples for natural risks are: <ul style="list-style-type: none"><li>Flooding</li><li>Avalanches</li></ul>	--
Eu.SecSpec.3100	Req	The IM shall choose the location considering industrial risks.	IM
Eu.SecSpec.3101	Info	Examples for industrial risks are: <ul style="list-style-type: none"><li>nuclear power plants</li><li>reservoirs/barriers</li><li>airfields/airports</li><li>chemical plants</li></ul>	--
Eu.SecSpec.2532	Req	The IM shall choose the location considering access to the location in case of major social events	IM
Eu.SecSpec.3102	Info	Major social events are for example: <ul style="list-style-type: none"><li>political events (strikes, demonstration, activist actions,...)</li><li>sports events</li><li>cultural events (concerts, botellón,...)</li></ul>	--
Eu.SecSpec.2533	Req	The IM shall choose the location considering prevention of attacks to the location in case of major social events	IM
Eu.SecSpec.3103	Info	Attacks by humans can originate for example from: <ul style="list-style-type: none"><li>political events (strikes, demonstration, activist actions,...)</li><li>sports events</li></ul>	--
Eu.SecSpec.2534	Head	<b>2.10.3 M00010: Rules for locations with minor importance</b>	
Eu.SecSpec.2795	Head	<b>2.10.3.1 General</b>	
Eu.SecSpec.2536	Info	Measure ID: M00010	--
Eu.SecSpec.2537	Info	Affected SuC: <ul style="list-style-type: none"><li>EfeS</li><li>SCS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.2541	Info	Threats: <ul style="list-style-type: none"><li>T 05 Natural Disasters</li><li>T 06 Environmental Disasters</li><li>T 024 Destruction of Devices or Storage Media</li><li>T 034 Attack</li></ul>	--
Eu.SecSpec.2546	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.2551	Req	The IM shall define rules for the location with respect of natural, environmental, and human-made disasters.	IM
Eu.SecSpec.2553	Head	<b>2.10.3.2 SCS</b>	
Eu.SecSpec.2554	Req	The IM shall define rules for the location of SCS components categorized as single points of failure.	IM
Eu.SecSpec.2555	Head	<b>2.10.4 M00008: Design components according to EN50125-3</b>	
Eu.SecSpec.2796	Head	<b>2.10.4.1 General</b>	
Eu.SecSpec.2557	Info	Measure ID: M00008	--

ID	Type	Requirement	Valid for
Eu.SecSpec.2558	Info	Affected SuC: <ul style="list-style-type: none"> <li>EfeS</li> <li>SCS</li> <li>ILS-Adapter</li> </ul>	--
Eu.SecSpec.2562	Info	Threats: <ul style="list-style-type: none"> <li>T 02 Unfavourable Climatic Conditions</li> <li>T 03 Water</li> <li>T 04 Pollution, Dust, Corrosion</li> <li>T 024 Destruction of Devices or Storage Media</li> <li>T 034 Attack</li> </ul>	--
Eu.SecSpec.2568	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>None</li> </ul>	--
Eu.SecSpec.2571	Req	The components installed at or near trackside shall be compliant with EN50125-3 (Railway applications - Environmental conditions for equipment - Part 3: Equipment for signalling and telecommunications).	All
Eu.SecSpec.2572	Head	<b>2.10.5 M00009: Design housing according to EN50600</b>	
Eu.SecSpec.2797	Head	<b>2.10.5.1 General</b>	
Eu.SecSpec.2574	Info	Measure ID: M00009	--
Eu.SecSpec.2575	Info	Affected SuC: <ul style="list-style-type: none"> <li>EIL</li> <li>MDM</li> <li>SSP</li> <li>ILS-Adapter</li> <li>SCS</li> </ul>	--
Eu.SecSpec.2580	Info	Threats: <ul style="list-style-type: none"> <li>T 01 Fire</li> <li>T 03 Water</li> <li>T 05 Natural Disasters</li> <li>T 06 Environmental Disasters</li> <li>T 07 Major Events in the Environment</li> <li>T 012 Interfering Radiation</li> <li>T 024 Destruction of Devices or Storage Media</li> <li>T 030 Unauthorised Use or Administration of Devices and Systems</li> <li>T 034 Attack</li> <li>T 041 Sabotage</li> <li>T 042 Social Engineering</li> <li>T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.2593	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>None</li> </ul>	--
Eu.SecSpec.2596	Req	The housing of the EIL shall be compliant to EN 50600 (Information technology - data centre facilities and infrastructures).	All
Eu.SecSpec.3105	Req	The housing of the MDM shall be compliant to EN 50600 (Information technology - data centre facilities and infrastructures).	All
Eu.SecSpec.3106	Req	The housing of the SSP shall be compliant to EN 50600 (Information technology - data centre facilities and infrastructures).	All
Eu.SecSpec.3107	Info	If the ILS-Adapter is located in the housing of the EIL, the ILS-Adapter is protected by the housing of the EIL.	--
Eu.SecSpec.2598	Req	The IM shall define the required availability class (EN 50600-1, table 1) based on the chosen overall system architecture (Grade of centralization).	IM
Eu.SecSpec.2604	Req	The housing of the Network Operation Centre (NOC) shall be compliant to EN 50600 (Information technology - data centre facilities and infrastructures).	All
Eu.SecSpec.3108	Req	The housing of network core elements shall be compliant to EN 50600 (Information technology - data centre facilities and infrastructures).	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2605	Head	<b>2.10.6 M00011: Design physical intrusion protection for shelter or cubicle</b>	
Eu.SecSpec.2798	Head	<b>2.10.6.1 General</b>	
Eu.SecSpec.2607	Info	Measure ID: M00011	--
Eu.SecSpec.2608	Info	Affected SuC: <ul style="list-style-type: none"><li>EfeS</li><li>SCS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.2611	Info	Threats: <ul style="list-style-type: none"><li>T 07 Major Events in the Environment</li><li>T 024 Destruction of Devices or Storage Media</li><li>T 034 Attack</li></ul>	--
Eu.SecSpec.2615	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.3109	Req	If the ILS-Adapter is located in the housing of the EIL, measure M00011 shall not be applied to the ILS-adapter.	All
Eu.SecSpec.3110	Req	If the ILS-Adapter is not located in the housing of the EIL, the IM shall use EN 50600 as a guideline.	IM
Eu.SecSpec.2619	Req	The shelter of the component shall conform to EN 1627 RC 1 N.	All
Eu.SecSpec.3111	Req	The cubicle of the component shall conform to EN 1627 RC 1 N.	All
Eu.SecSpec.2620	Req	The shelter of the component shall detect intrusion.	All
Eu.SecSpec.3112	Req	The cubicle of the component shall detect intrusion.	All
Eu.SecSpec.3113	Req	The housing's intrusion detection system shall report events to a centralized system.	All
Eu.SecSpec.3114	Req	The centralized system for intrusion detection shall provide events to either SSP-SLOG or directly the SIEM.	All
Eu.SecSpec.2621	Req	The shelter of the component shall restrict access using a physical access control system.	All
Eu.SecSpec.3115	Req	The cubicle of the component shall restrict access using a physical access control system.	All
Eu.SecSpec.3116	Req	The IM shall grant access to the shelter based on the least-privilege-principle.	IM
Eu.SecSpec.3117	Req	The IM shall grant access to the cubicle based on the least-privilege-principle.	IM
Eu.SecSpec.2623	Info	Intrusion detection events may be analysed and correlated with planned activities, e.g., maintenance.	--
Eu.SecSpec.2624	Head	<b>2.10.7 M00018: Electromagnetic Compatibility (EMC)</b>	
Eu.SecSpec.2799	Head	<b>2.10.7.1 General</b>	
Eu.SecSpec.2626	Info	Measure ID: M00018	--
Eu.SecSpec.2627	Info	Affected SuC: <ul style="list-style-type: none"><li>EfeS</li><li>ILS-Adapter</li></ul>	--
Eu.SecSpec.2630	Info	Threats: <ul style="list-style-type: none"><li>T 012 Interfering Radiation</li></ul>	--
Eu.SecSpec.2632	Info	Reference to IEC 62443: <ul style="list-style-type: none"><li>None</li></ul>	--
Eu.SecSpec.2635	Req	The components installed at or near trackside shall be conformant to EN 50121-4.	All



ID	Type	Requirement	Valid for
Eu.SecSpec.2637	Head	<b>2.10.8 M00032: Anti-Theft</b>	
Eu.SecSpec.2800	Head	<b>2.10.8.1 General</b>	
Eu.SecSpec.2639	Info	Measure ID: M00032	--
Eu.SecSpec.2640	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EIL</li> <li>• MDM</li> <li>• SSP</li> <li>• EfeS</li> <li>• SCS</li> <li>• ILS-Adapter</li> </ul>	--
Eu.SecSpec.2646	Info	Threats: <ul style="list-style-type: none"> <li>• T 016 Theft of Devices, Storage Media and Documents</li> <li>• T 017 Loss of Devices, Storage Media and Documents</li> <li>• T 024 Destruction of Devices or Storage Media</li> <li>• T 044 Unauthorised Entry to Premises</li> </ul>	--
Eu.SecSpec.2651	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2654	Req	The IM shall include theft and loss of the component and its related information in the ISMS and Supply Chain Security requirements	IM
Eu.SecSpec.3118	Info	An ISMS usually includes anti-theft of devices, storage medias and documents.	--
Eu.SecSpec.3119	Info	Theft of the components of the EIL, MDM and SCS (central components) are protected by the housing.	--
Eu.SecSpec.3120	Req	The IM shall define physical anti theft protection measures for the EfeS.	IM
Eu.SecSpec.3121	Req	The IM shall define physical anti theft protection measures for the decentralized SCS components.	IM
Eu.SecSpec.2655	Info	Depending on protection requirement, the removal or transport of the respective component should be made difficult. E.g., by attaching the component in a way that it cannot be easily removed; by storing or installing the component in a housing which cannot be removed with simple human force or simple tools.	--
Eu.SecSpec.2659	Head	<b>2.10.9 M00063: Physical protection of unprotected communication</b>	
Eu.SecSpec.2801	Head	<b>2.10.9.1 General</b>	
Eu.SecSpec.2661	Info	Measure ID: M00063	--
Eu.SecSpec.2662	Info	Affected SuC: <ul style="list-style-type: none"> <li>• EfeS</li> <li>• ILS-Adapter</li> <li>• TCS</li> <li>• RBC</li> </ul>	--
Eu.SecSpec.2667	Info	Threats: <ul style="list-style-type: none"> <li>• T 043 Replaying Messages</li> </ul>	--
Eu.SecSpec.2669	Info	Reference to IEC 62443: <ul style="list-style-type: none"> <li>• None</li> </ul>	--
Eu.SecSpec.2672	Req	If a cable is used to transmit data, not protected according to requirements for protection of confidentiality or integrity of data in transit, then the cable shall be physically protected.	All
Eu.SecSpec.3122	Req	If a connector to a cable or to a network device or to the component is used to transmit data, not protected according to requirements for protection of confidentiality or integrity of data in transit, then the connector shall be physically protected.	All
Eu.SecSpec.3123	Req	If a network device is used to transmit data, not protected according requirements for protection of confidentiality or integrity of data in transit, then the network device shall be physically protected.	All

ID	Type	Requirement	Valid for
Eu.SecSpec.2673	Info	The communication channel can be classified as physically protected if the surrounding equipment housing, cubicle, shelter or building is protected (inter alia M00002, M00008 and M00009 (for data centres) or M000011 (for cabinets and containers))	--