



EULYNX Initiative

Guideline for network architecture

Document number: Eu.Doc.25
Version: 1.3 (1.A)

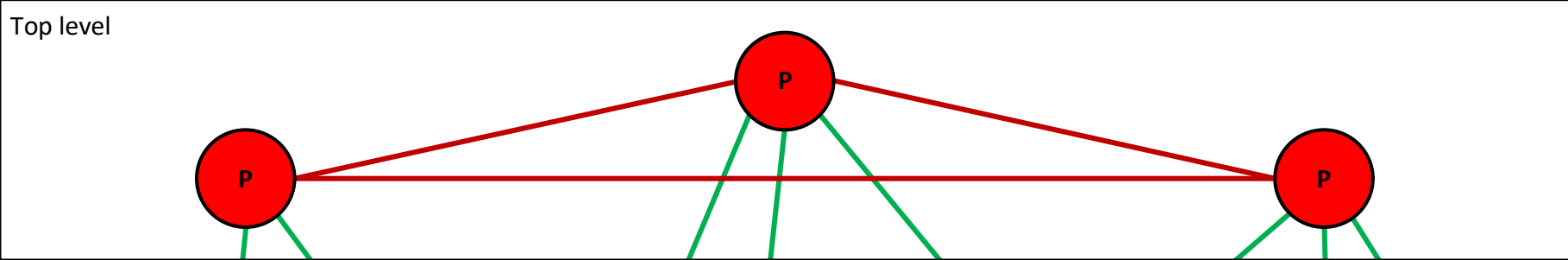
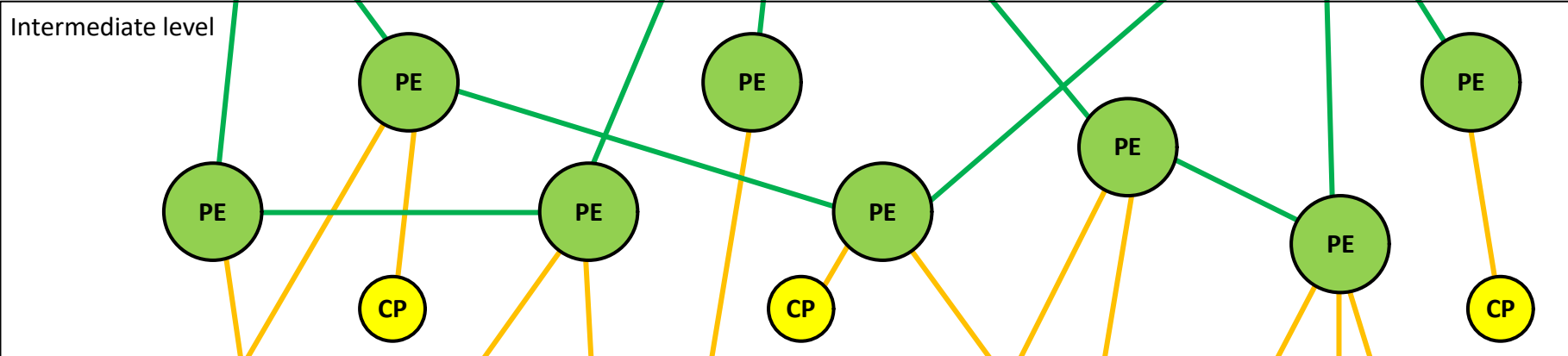
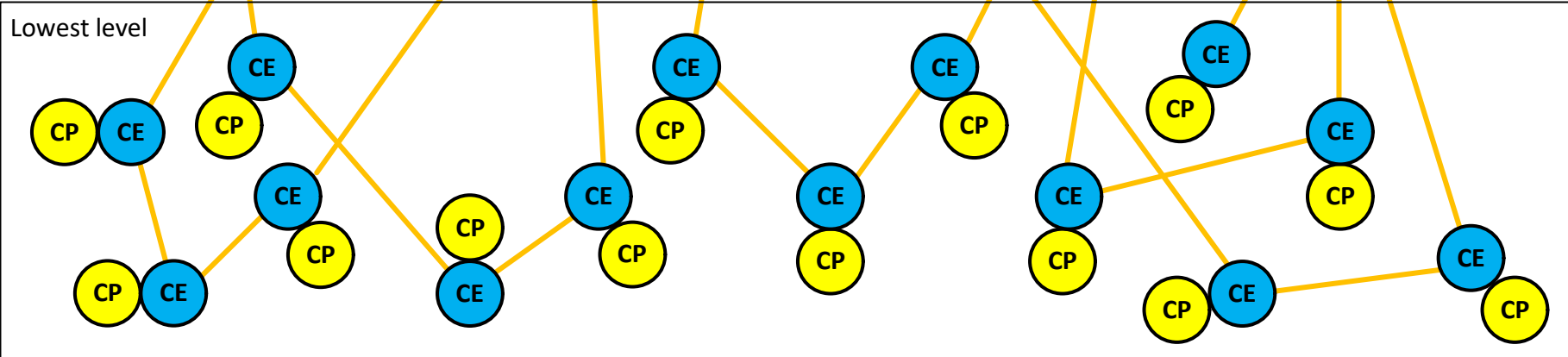
Contents

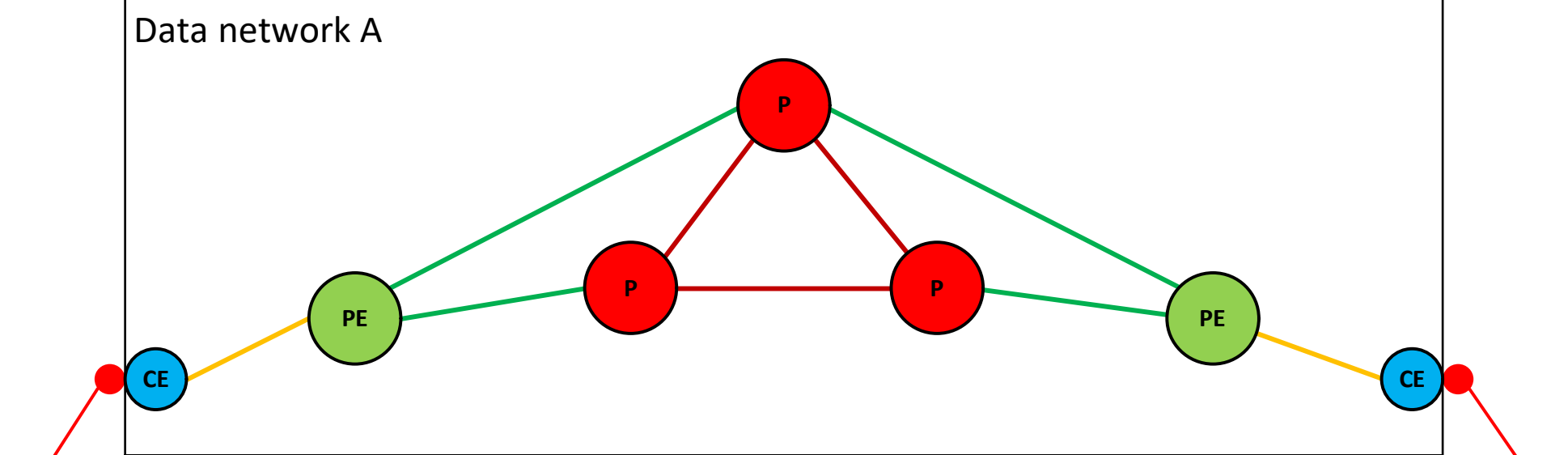
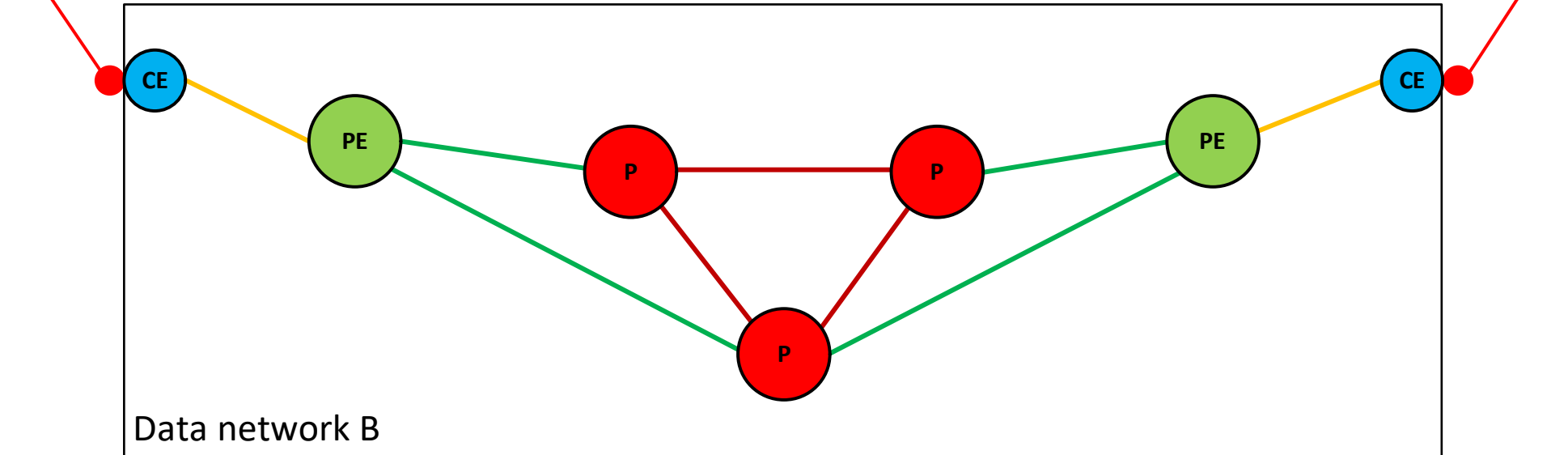
1	Introduction	1
1.1	Release information	1
1.2	Impressum	1
1.3	Purpose	2
1.4	Applicable standards and regulations	2
1.5	Applicable documents	2
1.6	Terms and abbreviations	2
1.7	Variability management	2
1.8	Definition of object types	2
2	Network hierarchy	3
3	Network plane redundancy	4
3.1	Two physically separated data networks	4
3.2	One data network with internal redundancy	5
4	Connecting communication participants	6
4.1	Cabling redundancy	8
5	Layer 2 vs. layer 3 connectivity	9
5.1	Routing in different hierarchy levels	9
6	Decomposition of communication paths	10
6.1	Security considerations related to communication paths	16
7	Responsibilities	17
8	Maintenance strategy	17

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.9	Head	1 Introduction		
Eu.Net.848	Head	1.1 Release information		
Eu.Net.948	Info	[Eu.Doc.25] Guideline for network architecture CENELEC Phase: 4 Version: 1.3 (1.A) Approval date: 29.05.2024		Object Text: [Eu.Doc.25] Guideline for network architecture CENELEC Phase: 4 Version: 1. 2 3 (2 1.A) Approval date: 15 29. 06 05. 2023 2024
Eu.Net.967	Info	Version history		
Eu.Net.1071	Info	version number: 1.0 (0.A) date: 13.12.2019 author: Nico Huurman, Jaco Schoonen review: CCB changes: EUAR-333, EUAR-335, EUAR-341		
Eu.Net.1072	Info	version number: 1.1 (0.A) date: 24.03.2022 author: Nico Huurman, Ulrich Meier review: cluster changes: EUAR-416, EUAR-461, EUAR-470, EUAR-483, EUAR-517		
Eu.Net.1089	Info	version number: 1.2 (0.A) date: 16.05.2022 author: Nico Huurman, Ulrich Meier review: CCB changes: EUAR-533		
Eu.Net.1090	Info	version number: 1.2 (1.A) date: 31.03.2023 author: Nico Huurman, Ulrich Meier review: changes: EUAR-540, EUAR-564		
Eu.Net.1091	Info	version number: 1.2 (2.A) date: 27.06.2023 author: Nico Huurman, Ulrich Meier review: CCB changes: EUAR-604, EUAR-613		
Eu.Net.1092	Info	version number: 1.3 (0.A) date: 29.04.2024 author: Nico Huurman review: cluster changes: EUAR-225, EUAR-681		object created after baseline 1.2 (2.A)
Eu.Net.1098	Info	version number: 1.3 (1.A) date: 18.06.2024 author: Nico Huurman review: CCB changes: EUAR-746		object created after baseline 1.2 (2.A)
Eu.Net.847	Head	1.2 Impressum		

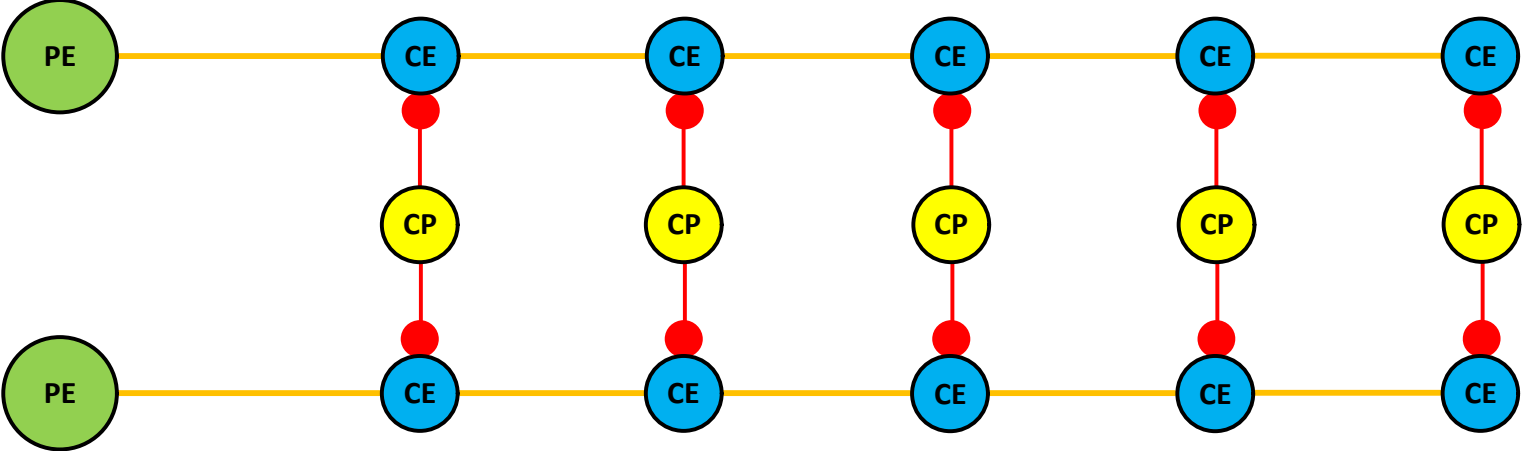
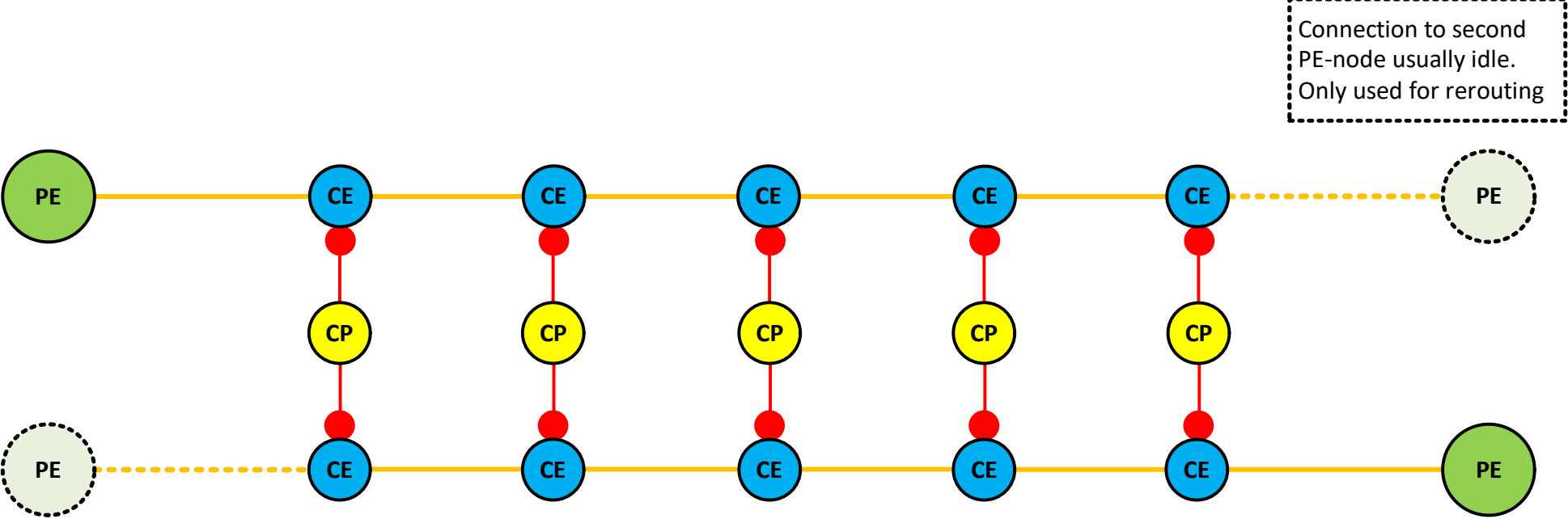
ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.946	Info	<p>Publisher: EULYNX Initiative</p> <p>A full list of the EULYNX Partners can be found on https://eulynx.eu/.</p>	EUAR-681	<p>Object Text: Publisher: EULYNX Initiative</p> <p>A full list of the EULYNX Partners can be found on www.https://eulynx.eu/index.php/members</p> <p>a_JIRA-Ticket BL4R3: EUAR-681</p>
Eu.Net.945	Info	<p>Responsible for this document: EULYNX Project Management Office www.eulynx.eu</p>		
Eu.Net.949	Info	<p>Copyright EULYNX Partners</p> <p>All information included or disclosed in this document is licensed under the European Union Public Licence EUPL, Version 1.2 or later.</p>		
Eu.Net.846	Head	1.3 Purpose		
Eu.Net.989	Info	This document is an informational guideline describing possible options and some of their properties to implement the data networks that form the Subsystem – Communication System.		
Eu.Net.990	Info	<p>The implementation of the Subsystem - Communication System shall be defined by national specifications.</p> <p>The concrete implementation may differ significantly from the options presented herein.</p>		
Eu.Net.991	Info	The national specific implementation of the Subsystem – Communication System consists of one or more data networks. This guideline can serve as input for infrastructure managers to define their requirements for the data networks that form the Subsystem - Communication System.		
Eu.Net.1088	Info	The Specification of Point of Service-Signalling [Eu.Doc.100] contains the list of requirements for the Subsystem - Communication System and is the baseline to assess whether the concrete network implementation is compliant or not.		
Eu.Net.845	Head	1.4 Applicable standards and regulations		
Eu.Net.940	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].		
Eu.Net.969	Head	1.5 Applicable documents		
Eu.Net.970	Info	The current versions of documents used as input or related to this document are listed in the EULYNX Documentation Plan [Eu.Doc.11]. The relationships between the documents are displayed in the Appendix A1 Documentation plan and structure [Eu.Doc.11_A1].		
Eu.Net.844	Head	1.6 Terms and abbreviations		
Eu.Net.893	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].		
Eu.Net.976	Head	1.7 Variability management		
Eu.Net.977	Info	This document is valid for the complete EULYNX System. Variability management is not used in this document. The specific applicability of requirements is captured in individual Requirements specifications. In implementation projects that apply the EULYNX specifications, it is possible to implement only parts of the architecture of the EULYNX System described in this document. The Infrastructure Manager initiating an implementation project, can use project documentation to indicate which parts of the architecture of the EULYNX System are applicable in a specific project.		
Eu.Net.972	Head	1.8 Definition of object types		
Eu.Net.947	Info	The following definition for object types is applied in this document:		
Eu.Net.973	Info	• "Req" - This denotes a mandatory requirement.		
Eu.Net.974	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.		
Eu.Net.975	Info	• "Head" - This denotes chapter headings.		

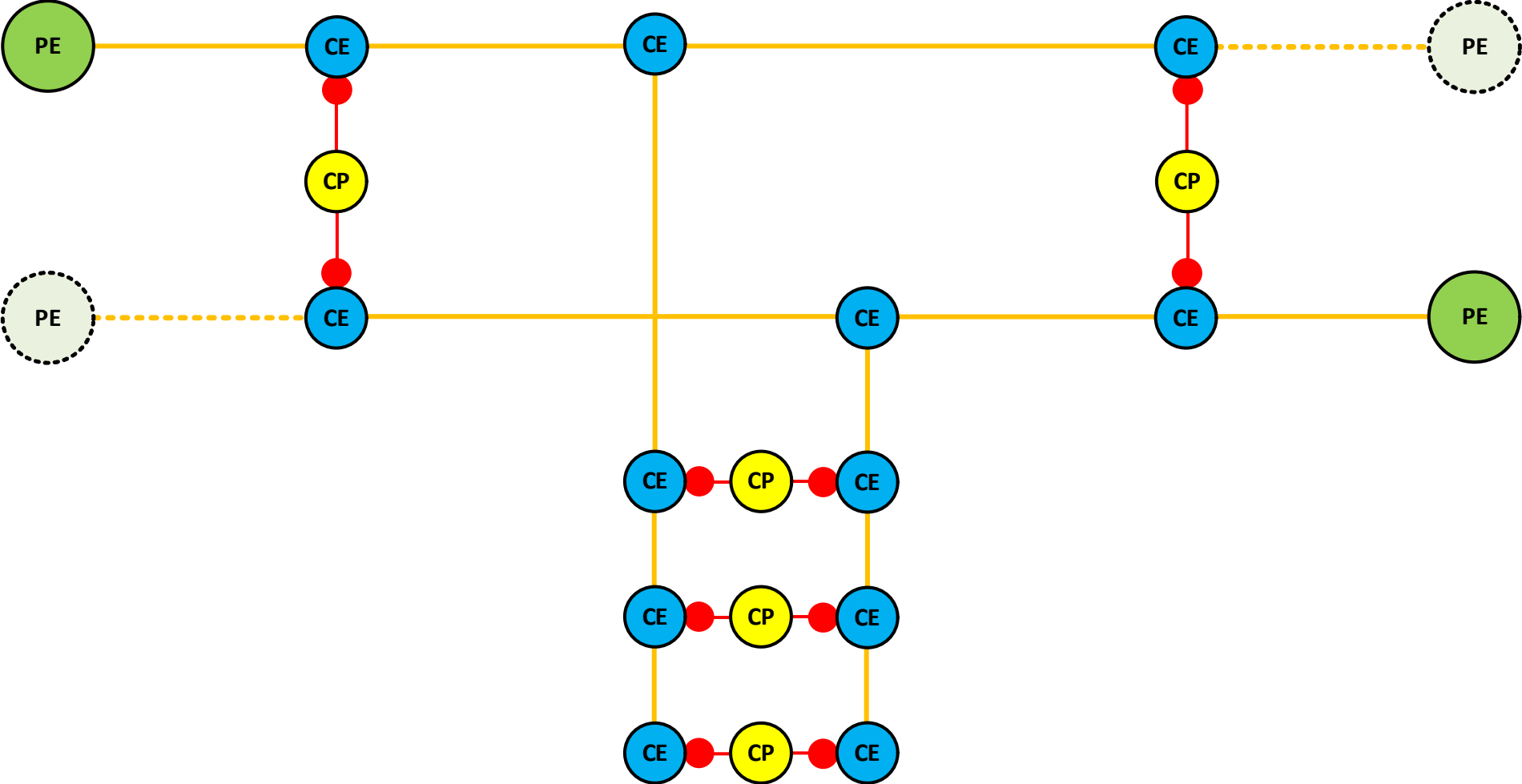
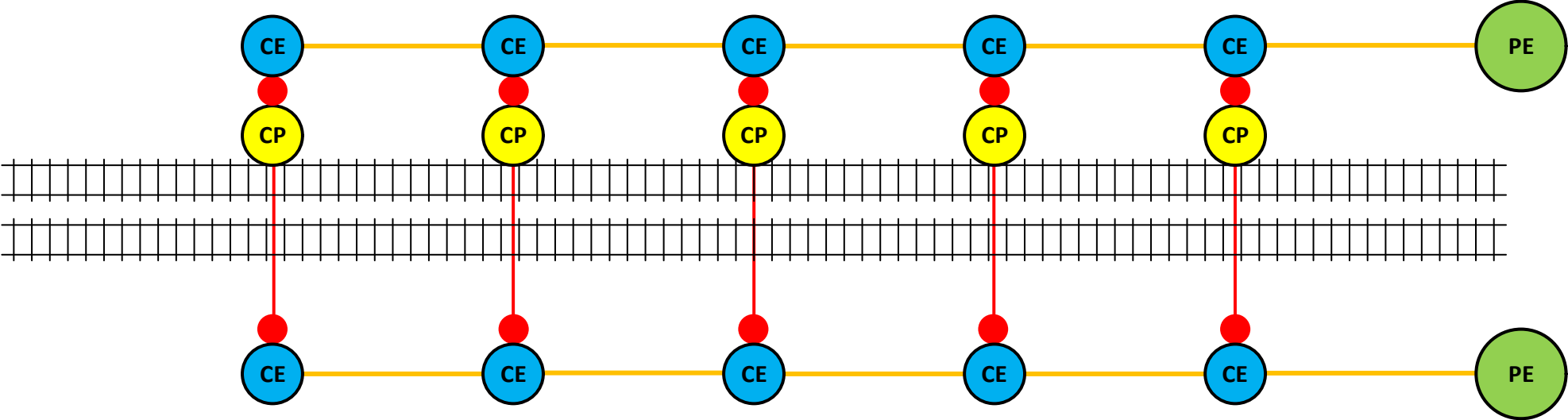
ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.992	Head	2 Network hierarchy		
Eu.Net.993	Info	A data network contains hierarchy in its architecture.		
Eu.Net.994	Info	The highest layer of the network hierarchy is recommended for large scale networks. This consists of provider nodes (P-nodes), which forms interconnections on a geographical scale for the data network that serves the IMs rail network.		
Eu.Net.995	Info	An intermediate layer of the network hierarchy connects P-nodes to provider edge nodes (PE-nodes). It also connects PE-nodes to each other.		
Eu.Net.996	Info	The lowest layer of the network hierarchy connects PE-nodes to customer edge nodes (CE-nodes). It may also connect CE-nodes to each other.		
Eu.Net.997	Info	A network architecture may also contain more than three hierarchy layers, having more than one intermediate layer or more than one customer edge layer. Traffic flow must never go down a layer and back up, e.g. traffic flow between PE-nodes must not traverse any CE-nodes.		
Eu.Net.998	Info	Communication participants (CP) are usually connected to CE-nodes at the lowest level of the network hierarchy.		
Eu.Net.999	Info	Communication participants that are located on central locations may be connected to the network on hierarchy layers that are above the lowest layer, e.g. directly to a PE-node. This may be valid for an electronic interlocking, that is located inside a data centre, not along a railway line. Note: National network specification may allow or disallow directly connecting communication participants to PE-nodes. If this is not allowed, a CE-node can be put in between a single communication participants and the PE-node.		

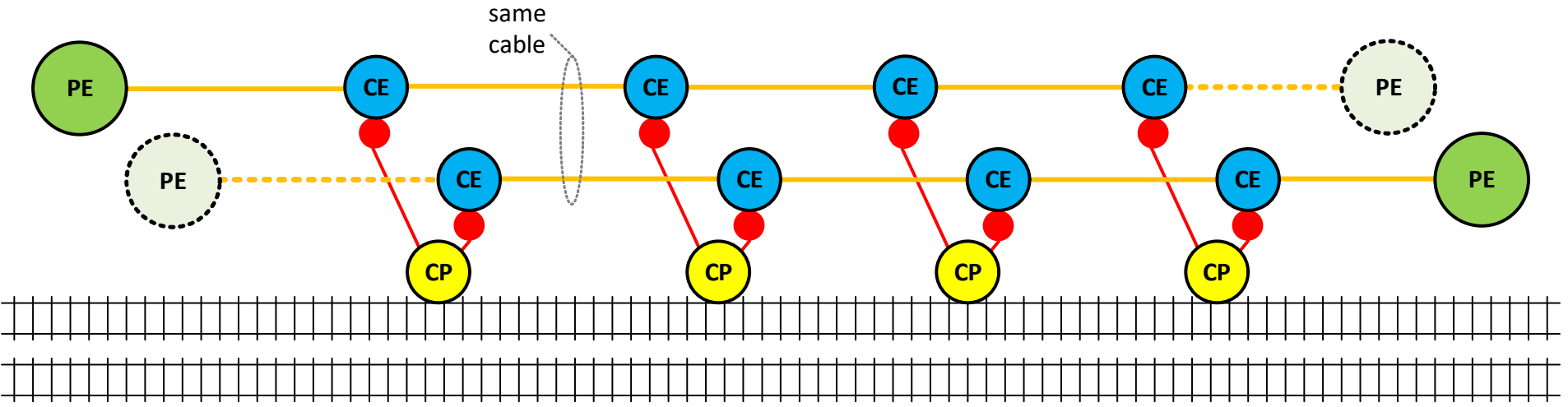
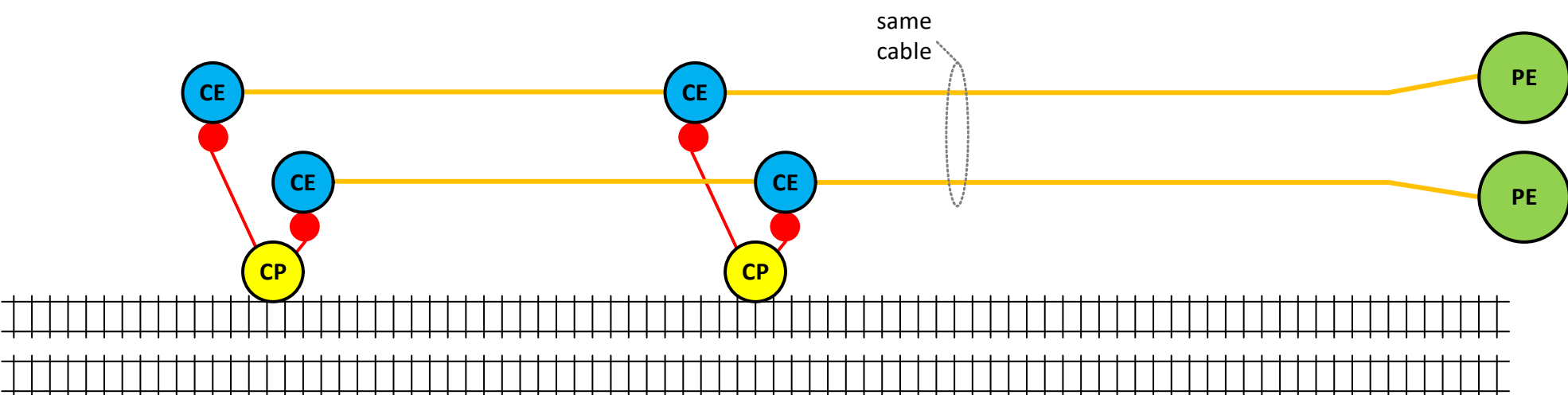
ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1000	Info	<div>Schematic representation of multi-layer network architecture</div> <div><div>Top level</div><div>Intermediate level</div><div>Lowest level</div></div>		
Eu.Net.1001	Head	3 Network plane redundancy		
Eu.Net.1004	Info	As required in [Eu.Doc.100], the network architecture must ensure that the Subsystem - Communication System can provide two independent network interfaces to each communication participant.		
Eu.Net.1005	Info	To ensure independent network interfaces, the network architecture must enable independent paths through the data network between two PoS-Signalling.		
Eu.Net.1006	Info	The independence of paths can be reached by providing two physically separated data networks or by providing one data network with internal redundancy.		
Eu.Net.1007	Info	Both principles can also be mixed in the network architecture. For example one data networks with internal redundancy can be provided on the highest hierarchy layer, while two physically separated data networks exist on the lower hierarchy layers.		
Eu.Net.1002	Head	3.1 Two physically separated data networks		
Eu.Net.1008	Info	In this implementation, each communication participant has a diverse connection to two independent data networks via a redundant implementation of the PoS-Signalling.		
Eu.Net.1009	Info	There is no connection between the active components of the two separated data networks.		
Eu.Net.1010	Info	Active components and connections inside one of the two data network nodes don't need to be implemented redundantly.		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1011	Info	It is acceptable that the failure of a single active component or connection inside one of the two data network interrupts the logical connection between two communication participants in that data network. The logical connection via the other data network remains undisturbed.		
Eu.Net.1012	Info	<div><div>Schematic representation of two physically separated data networks</div><div><div><div>Data network A</div><div>Data network B</div></div></div></div>		
Eu.Net.1003	Head	3.2 One data network with internal redundancy		
Eu.Net.1013	Info	In this implementation, at least the highest hierarchy level of the network architecture consists of only one data network.		
Eu.Net.1014	Info	The topology of active components and connections between them is such, that at least two independent paths can be provided between any two communication participants.		
Eu.Net.1015	Info	If an active component or connection fails, at least one alternative path through the data network must remain undisturbed.		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1016	Info	<div>Schematic representation of data network with internal redundancy</div> <div></div>		
Eu.Net.1017	Head	4 Connecting communication participants		
Eu.Net.1018	Info	Communication participants must be connected to the network via two independent network interfaces, as described in Eu.Net.1004. The upstream network must provide at least two independent paths, as described in Eu.Net.1014.		
Eu.Net.1019	Info	The implementation of the connection of a communication participant to the Subsystem - Communication System depends on the geographical location of the communication participant.		
Eu.Net.1020	Info	<p>1. Communication participants that are located in the direct vicinity of PE-nodes (i.e. inside the same room or building), may be connected to these intermediate nodes directly. To ensure redundancy, they must be connected to two independent nodes (PE/PE or PE/CE).</p> <p>Note: National network specification may allow or disallow directly connecting communication participants to PE-nodes. If this is not allowed, a CE-node can be put in between a single communication participants and the PE-node.</p>		
Eu.Net.1023	Info	This type of connection is usually applicable for central communication participants, like the Subsystem - Electronic Interlocking, the Subsystem - Maintenance and Data Management or adjacent systems.		
Eu.Net.1021	Info	<div>Implementation type 1, without or with intermediate CE-nodes.</div> <div></div>		
Eu.Net.1022	Info	2. Communication participants that are located in the station area of a station that also contains a PE-node, may be connected via a local sub-network for this station. To ensure redundancy, the sub-network must be connected to two independent PE-nodes.		



















ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1024	Info	This type of connection is usually applicable for object controllers of field elements in station areas of bigger stations.		
Eu.Net.1025	Info	<div>Implementation type 2</div> 		
Eu.Net.1026	Info	3. Communication participants that are located along a railway line, may be connected via a sub-network that runs along the railway line (see section 'Cabling redundancy'). This sub-network starts at a station with a PE-node and runs until the next station with a PE-node, thereby connecting to two independent PE-nodes.		
Eu.Net.1027	Info	To further increase the redundancy, the sub-network may be connected to two PE-nodes on each end. In this case, only one of the two connections to PE-nodes is in active use in normal situations. Only when the network is interrupted somewhere along the railway line, traffic can be re-routed to also use the second PE-nodes on both ends.		
Eu.Net.1028	Info	This type of connection is usually applicable for object controllers of remotely located single field elements.		
Eu.Net.1029	Info	<div>Implementation type 3</div> 		
Eu.Net.1030	Info	4. Communication participants that are located in the station area of a remote station, may be connected via a local sub-sub-network for this station, connected to the sub-network that runs along the railway line.		
Eu.Net.1031	Info	This type of connection is usually applicable for object controllers of a group of remotely located field elements.		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1032	Info	<div>Implementation type 4</div> 		
Eu.Net.1033	Head	4.1 Cabling redundancy		
Eu.Net.1034	Info	The independence of two network interfaces must also be maintained when connecting communication participants that are located on remote locations along railway lines (e.g. object controllers of signals or points located far away from stations).		
Eu.Net.1035	Info	The cabling configuration to connect these remote communication participants must be redundant. This can be realised in different ways.		
Eu.Net.1036	Info	1. Two cables can be used between a redundant intermediate network node and remote communication participants, with one on each side of the railway line.		
Eu.Net.1037	Info	If the cable on one side would get damaged on a certain spot, the cable on the other side of the railway line still ensures the connection.		
Eu.Net.1038	Info	<div>Cabling configuration 1</div> 		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1039	Info	2. One cable can be used on one side of the railway line. This cable connects an intermediate network node to communication participants and continues along the railway line until reaching another intermediate network node.		
Eu.Net.1040	Info	If the cable would get damaged on a certain spot, the continuation of the cable towards the next intermediate network node still ensures the connection.		
Eu.Net.1041	Info	<p>Cabling configuration 2</p> 		
Eu.Net.1042	Info	3. Both logical connections can be using different fibres all placed in a single cable, to reach remote communication participants. National specifications regarding availability must determine the maximum length for which such a configuration is acceptable.		
Eu.Net.1043	Info	If the fibres of one of the two logical connections inside the cable would get damaged, the fibres of the other logical connection can still ensure the communication. If the cable itself would get damaged, the affected communication participants are no longer connected to the network.		
Eu.Net.1044	Info	<p>Cabling configuration 3</p> 		
Eu.Net.1045	Head	5 Layer 2 vs. layer 3 connectivity		
Eu.Net.1046	Info	Connectivity may be provided at both layer 2 (Data link layer) and layer 3 (Network layer).		
Eu.Net.1067	Info	Layer 3 connectivity is the common way to build a geographically distributed network. This may, however, require additional routing information to be configured in the application to fully support redundant connections.		
Eu.Net.1068	Info	Layer 2 connectivity is easier to configure. However, providing layer 2 connectivity on a geographically distributed network may make it more difficult to maintain a stable network. To avoid address resolution issues, layer 2 domains should not be too large.		
Eu.Net.1069	Info	The EULYNX communication participants support both layer 2 and 3 connectivity. The connectivity provided by the Subsystem - Communication System may be defined by national specifications.		
Eu.Net.1047	Head	5.1 Routing in different hierarchy levels		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)																																																																		
Eu.Net.1048	Info	In a layer 2 network all communication participants are connected at the data link layer. Therefore, no routing has to be configured in the network stack of the communication participants. Typically, this is only used in local area networks. There are nowadays techniques (e.g. EVPN or PBB-EVPN) that provide the behaviour of LAN-connectivity also on a geographically distributed network.																																																																				
Eu.Net.1070	Info	If a layer 3 network is used, typically a default gateway is used to route traffic to unknown addresses. However, by doing this the communication participant routes all traffic over a single interface as there can only be one default gateway. This is not in line with having two independent communication channels and can be solved by adding static routing configuration in the communication participant to route certain IP-ranges to different network interfaces.																																																																				
Eu.Net.1073	Head	6 Decomposition of communication paths																																																																				
Eu.Net.1074	Info	The purpose of the following figures is to have a common setting and identification of points related to communication.																																																																				
Eu.Net.1075	Info	<div>Explanation of IDs used in the figures:<table><tr><th>ID</th><th>Description</th><th>Remarks</th></tr><tr><td>A</td><td>EULYNX field element Subsystem (EfeS)</td><td></td></tr><tr><td>B</td><td colspan="2">TLS hardware board or software component (variant B/C)</td></tr><tr><td>C</td><td>Crypto box (variant A): EfeS version</td><td></td></tr><tr><td>D</td><td colspan="2">Crypto box (variant A): data centre version</td></tr><tr><td>E</td><td>Firewall "complex": ALG</td><td></td></tr><tr><td>F</td><td colspan="2">Firewall "simple": ports, addresses, standard protocols</td></tr><tr><td>G</td><td>Connection Manager</td><td>terminates TLS in front of EIL (cleartext or TLS between G and I); SCI protocol translation between multiple EULYNX base lines; may terminate RaSTA (proprietary protocol between G and I)</td></tr><tr><td>H</td><td>TLS termination</td><td></td></tr><tr><td>I</td><td>EIL</td><td></td></tr><tr><td>L</td><td>MDM</td><td></td></tr><tr><td>M</td><td>Security Service Platform (SSP)</td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td colspan="2">Communication system</td><td></td></tr><tr><td>a</td><td>Switch in cabinet ("last mile")</td><td></td></tr><tr><td>b</td><td>Switch in container, house ("last mile")</td><td></td></tr><tr><td>c</td><td colspan="2">Provider Edge (PE) component ("entry to regional or core network")</td></tr><tr><td>d</td><td>Mobile Network access point</td><td>includes switch and VLAN/QoS support</td></tr><tr><td>e</td><td colspan="2">Radio base station / RAN (Mobile Network A)</td></tr><tr><td>f</td><td colspan="2">Interconnection mobile network A to communication network</td></tr><tr><td>g</td><td colspan="2">Radio base station / RAN (Mobile Network B)</td></tr><tr><td>h</td><td colspan="2">Interconnection mobile network B to communication network</td></tr></table></div>	ID	Description	Remarks	A	EULYNX field element Subsystem (EfeS)		B	TLS hardware board or software component (variant B/C)		C	Crypto box (variant A): EfeS version		D	Crypto box (variant A): data centre version		E	Firewall "complex": ALG		F	Firewall "simple": ports, addresses, standard protocols		G	Connection Manager	terminates TLS in front of EIL (cleartext or TLS between G and I); SCI protocol translation between multiple EULYNX base lines; may terminate RaSTA (proprietary protocol between G and I)	H	TLS termination		I	EIL		L	MDM		M	Security Service Platform (SSP)					Communication system			a	Switch in cabinet ("last mile")		b	Switch in container, house ("last mile")		c	Provider Edge (PE) component ("entry to regional or core network")		d	Mobile Network access point	includes switch and VLAN/QoS support	e	Radio base station / RAN (Mobile Network A)		f	Interconnection mobile network A to communication network		g	Radio base station / RAN (Mobile Network B)		h	Interconnection mobile network B to communication network			
ID	Description	Remarks																																																																				
A	EULYNX field element Subsystem (EfeS)																																																																					
B	TLS hardware board or software component (variant B/C)																																																																					
C	Crypto box (variant A): EfeS version																																																																					
D	Crypto box (variant A): data centre version																																																																					
E	Firewall "complex": ALG																																																																					
F	Firewall "simple": ports, addresses, standard protocols																																																																					
G	Connection Manager	terminates TLS in front of EIL (cleartext or TLS between G and I); SCI protocol translation between multiple EULYNX base lines; may terminate RaSTA (proprietary protocol between G and I)																																																																				
H	TLS termination																																																																					
I	EIL																																																																					
L	MDM																																																																					
M	Security Service Platform (SSP)																																																																					
Communication system																																																																						
a	Switch in cabinet ("last mile")																																																																					
b	Switch in container, house ("last mile")																																																																					
c	Provider Edge (PE) component ("entry to regional or core network")																																																																					
d	Mobile Network access point	includes switch and VLAN/QoS support																																																																				
e	Radio base station / RAN (Mobile Network A)																																																																					
f	Interconnection mobile network A to communication network																																																																					
g	Radio base station / RAN (Mobile Network B)																																																																					
h	Interconnection mobile network B to communication network																																																																					
Eu.Net.1076	Info		EUAR-746	a_JIRA-Ticket BL4R3: EUAR-746																																																																		

ID	Type	Requirement		JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1076		ID	Description	Remarks	
		Interfaces / Ports			
		1	SCI, EfeS: RaSTA to transport adaption using TLS/TCP		
		2	SCI, EfeS: RaSTA to transport adaption using UDP		
		7	SSI: EIL, EfeS, MDM		
		8	SMI: EfeS, EIL		
		9	SDI: EfeS, EIL		
		10	SCS: used for variant A (Crypto box, EfeS version)		
		11	SCS: used for TLS (variant B/C)		
		12	SCS: fixed mobile, used for TLS (variant B/C)		
		14	SCS: used for cat 2 network		
		15	SCS: cabinet, trackside network		
		16	SCS: mobile network interface (radio), terminal		
		17	SCS: mobile network interface (radio), base station		
		18	SCS: concentrator, trackside network "last mile"		
		19	SCS: trackside network "last mile" to provider edge		
		20	SCS: provider edge interface to core network		
		21	SCS: provider edge to trackside network "last mile"		
		22	SCS: Interface to data centre		
		25	SCS: base station to mobile core network provider A		
		26	SCS: base station to mobile core network provider B		
		27	SCS: mobile core network provider A to interconnection to wire-base network		
		28	SCS: mobile core network provider B to interconnection to wire-base network		
		30	SCI, EIL: RaSTA to transport adaption using TLS/TCP		
		31	SCI, EIL: RaSTA to transport adaption using UDP		
		32	SCI, EIL: SCI to RaSTA	pure SCI, non-EULNYX	
		37	SSI, SSP		
		38	SMI, MDM		
		39	SDI, MDM		
		40	Crypto box to EfeS		
		41	Crypto box to communication system		
		50	Crypto box to communication system		
		51	Crypto box to data centre		
Eu.Net.1077	Info				

ID	Type	Requirement			JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1077		ID	Description	Remarks		
		60	Firewall from external			
		61	Firewall to SCI			
		67	Firewall to SSI			
		68	Firewall to SMI			
		69	Firewall to SDI			
		70	RaSTA: Transport adaption, OC side			
		71	TLS/TCP to SCS, wire base			
		72	TLS/TCP to SCS, fixed mobile			
		73	TLS/TCP to SCS, using integrated mobile	for assurance/certification this must be observable		
		80	SCS to TLS/TCP			
		81	Transport adaption to RaSTA, EIL side			
		90	SCI, towards SCS; TLS encrypted	SCI over RaSTA over TLS/TCP		
		91	SCI, towards EIL; TLS encrypted	SCI over RaSTA over TLS/TCP		
		92	SCI, towards SCS; not encrypted (requires cat 2)	SCI over RaSTA over UDP		
		93	SCI, towards EIL; not encrypted (requires cat 2)	SCI over RaSTA over UDP		
		94	SCI, towards EIL; not encrypted, non-EULYNX	SCI, not using RaSTA (connection controller terminates RaSTA, connection manager is part of EIL for safety assessment)		
		101	generic use device with IP	e.g. climate control, energy management, intrusion detection, fire alarm,...		
		102	non-EULYNX to communication system			
		103	non-EULYNX to communication system			
Eu.Net.1079	Info	All figures use the following colour schema and the following symbols				
		 SCI  SSI  non-EULYNX  physical				
		 SMI  Communication System  NAC: EAP-TLS or SIM card				
		 SDI  Security  Encryption				
		 Network (SCS)  Router (SCS)  Switch (not SCS)				
		 Switch (SCS)  Firewall				
		 Network (mobile operator)  Gateway (mobile operator)  Mobile				

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1080	Info	<p>For the situation using a pure category 2 network [EN 50159:2010], the following figure applies for a single pane setup. The multi pane setup is double.</p>		
Eu.Net.1081	Info	<p>For the situation using "Crypto box" (variant A) the following figure applies. Note: Details on the "Crypto box" variant are documented in the EULYNX Security Concept [Eu.Doc.15].</p>	EUAR-746	<p>Object Text: For the situation using "cryptoboxCrypto box" (variant A) the following figure applies. Note: Details on the "cryptoboxCrypto box" variant are documented in the EULYNX Security Concept [Eu.Doc.15]. a_JIRA-Ticket BL4R3: EUAR-746</p>

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1078	Info	For situation using TLS/TCP variants multiple figures apply. a) without using "connection manager" b) using "connection manager" c) combined wire-based and mobile connection of EfeS (fixed mobile access point is used) d) mobile only for EfeS with fixed mobile (access points) e) mobile only for EfeS with integrated mobile		
Eu.Net.1082	Info	Details on TLS/TCP variants are documented in the EULYNX Security Concept [Eu.Doc.15], the EULYNX Security Specifications [Eu.Doc.114] and the EULYNX Security Parameter Specification [Eu.Doc.115].		
Eu.Net.1084	Info	<p>TLS/TCP without "connection manger"</p> <p>The diagram illustrates a network architecture for TLS/TCP without a connection manager. It is divided into three main sections: Cabinet, Container/House, and Data center. The Cabinet section shows a central node (101) connected to a group of nodes (1, 7, 8, 9) and a TLS node (71). The Container/House section shows a central node (102) connected to a group of nodes (11, 15, 18, 19, 21, 20) and a PE node (20). The Data center section shows a central node (103) connected to a group of nodes (61, 67, 68, 69, 80, 81, 30, 7, 8, 9) and a TLS node (81). The Data center also includes a Firewall node (60) and a group of nodes (38, 39, 37) labeled L, M, and SSP. The diagram uses various icons to represent different components, such as locks for security and server racks for hardware.</p>		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1086	Info	<p>TLS/TCP with mobile only for EfeS with fixed mobile (access points). Note: May be combined with connection manager.</p>		
Eu.Net.1087	Info	<p>TLS/TCP with mobile only for EfeS with integrated mobile. Note: May be combined with connection manager.</p>		
Eu.Net.1093	Head	6.1 Security considerations related to communication paths	EUAR-225	object created after baseline 1.2 (2.A)

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1094	Info	The security risk assessment for EULYNX does not include direct communication paths between two EULYNX field element Subsystems. It assumes that all communication paths have a centrally located device as at least one of the two communication partners. This can be e.g. the Subsystem - Electronic Interlocking, the Subsystem - Maintenance and Data Management or adjacent systems.	EUAR-225	object created after baseline 1.2 (2.A)
Eu.Net.1095	Info	Use of direct communication paths between two EULYNX field element Subsystems requires the consent of the operator, after a review of the security risk analysis.	EUAR-225	object created after baseline 1.2 (2.A)
Eu.Net.1096	Info	An example of a communication patch between two EULYNX field element Subsystems can be the exchange of information between two object controllers handling axle counters.	EUAR-225	object created after baseline 1.2 (2.A)
Eu.Net.1097	Info	Measures addressing security hazards may be needed to ensure compliance with the security risk assessment for EULYNX. This may include e.g.: <ul style="list-style-type: none"> • Protocol stack used for the communication • Hardening of the communication partners • Routing of the communication path 	EUAR-225	object created after baseline 1.2 (2.A)
Eu.Net.1049	Head	7 Responsibilities		
Eu.Net.1050	Info	The Subsystem - Communication System plays an important role in the EULYNX architecture of a signalling system.		
Eu.Net.1051	Info	The signalling system logically falls under the responsibility of the signalling department of an IM.		
Eu.Net.1052	Info	The data network(s) that implement the Subsystem - Communication System usually fall under the responsibility of the communication department of an IM.		
Eu.Net.1053	Info	To ensure smooth cooperation between these two department, enabling effective design, operation and maintenance of the Subsystem - Communication System, a clear division of responsibilities has to be agreed upon.		
Eu.Net.1054	Info	The Point of Service - Signalling can be used as a physical limit of responsibilities. Its basic physical and functional properties are defined in the Specification of Point of Service - Signalling [Eu.Doc.100].		
Eu.Net.1055	Info	Additional national specifications can be used to complete the requirements contained in [Eu.Doc.100].		
Eu.Net.1056	Head	8 Maintenance strategy		
Eu.Net.1057	Info	The redundancy that must be included in the network architecture of the Subsystem - Communication System can also be used to facilitate maintenance.		
Eu.Net.1058	Info	The network architecture can be designed such that it contains more than minimum level of redundancy that is necessary to provide a redundant and diverse implementation of the PoS-Signalling to communication participants [see Eu.Doc.100].		
Eu.Net.1059	Info	A network component can be taken offline for maintenance purposes without limitations, if the network architecture can still provide two diverse paths through the data network(s) that implement the Subsystem - Communication System without that network component.		

ID	Type	Requirement	JIRA	V 1.3 (1.A) > V 1.2 (2.A)
Eu.Net.1060	Info	<p>Example of rerouting during maintenance, using additional redundancy.</p> <p>Offline for maintenance</p> <p>same cable</p> <p>Connection to second PE-node usually idle. Only used for rerouting.</p> <p>Traffic rerouted to second PE-node.</p>		
Eu.Net.1061	Info	The network architecture probably can't provide sufficient additional redundancy to enable unlimited maintenance for all network components. The desired degree of unlimited maintenance is a complex cost vs. efficiency calculation and should be considered when designing the network.		
Eu.Net.1062	Info	Under appropriate conditions, it is still possible to take network components offline, even if this means it is no longer possible to provide two diverse paths through the data network(s). This can only be allowed when the affected communication participants have a functioning redundant network interface.		
Eu.Net.1063	Info	An analysis that takes into account the national specifications for availability of the PoS-Signalling will define the acceptable boundary conditions for such network components offline.		
Eu.Net.1064	Info	Examples of boundary conditions can be: <ul style="list-style-type: none">• Limited duration of offline time• Offline time only allowed during low traffic periods• Offline time only allowed when additional repair teams are on standby		