EULYNX Initiative

Europe's Rail Joint Undertaking

Interface definition SCI

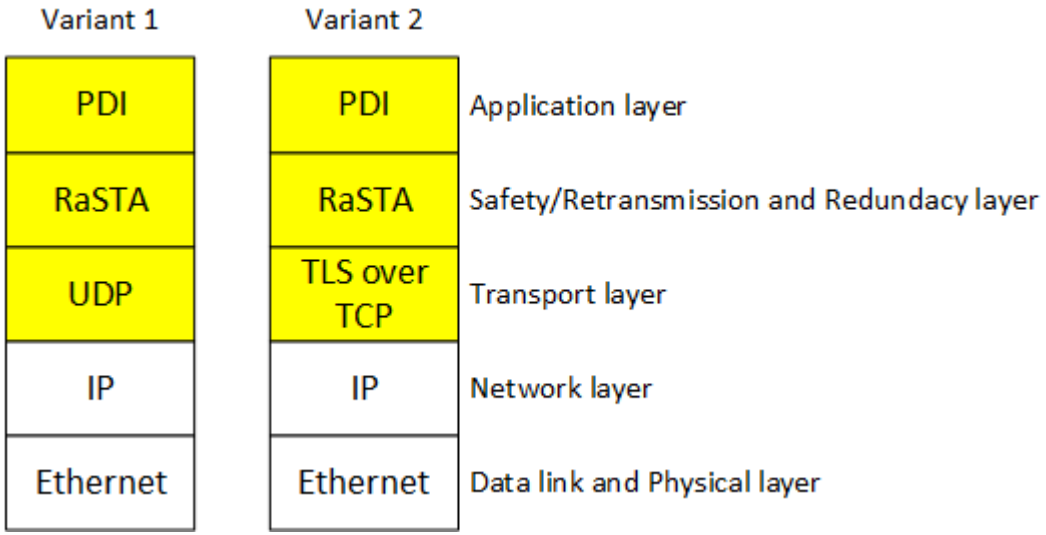
Document number: Eu.Doc.92
Version: 4.2 (0.A)

Contents

ID	Type	Requirement
Eu.SCI.6	Head	# 1 Introduction
Eu.SCI.7	Head	## 1.1 Release information
Eu.SCI.8	Info	[Eu.Doc.92] Interface definition SCI CENELEC Phase: 5 Version: 4.2 (0.A) Approval date: 15.06.2023
Eu.SCI.9	Info	**Version history**
Eu.SCI.245	Info	version number: 4.0 (0.A) date: 17.05.2022 author: Nico Huurman, package 4 working group review: CCB changes: EUAR-508, EUAR-526, EUAR-530
Eu.SCI.248	Info	version number: 4.1 (0.A) date: 31.03.2023 author: Nico Huurman review: changes: EUAR-545, EUAR-564, EUAR-571, EUAR-575
Eu.SCI.253	Info	version number: 4.1 (1.A) date: 10.05.2023 author: Nico Huurman review: cluster changes: EUAR-589
Eu.SCI.255	Info	version number: 4.2 (0.A) date: 27.06.2023 author: Nico Huurman review: TACS Mirror Group changes: EUAR-594, EUAR-610, EUAR-612, EUAR-613
Eu.SCI.11	Head	## 1.2 Impressum

ID	Type	Requirement
Eu.SCI.12	Info	Publishers: **Europe's Rail Joint Undertaking** https://rail-research.europa.eu **EULYNX Initiative** A full list of the **EULYNX Partners** can be found on www.eulynx.eu/index.php/members
Eu.SCI.13	Info	Responsible for this document: EU-Rail System Pillar Transversal CCS Components domain
Eu.SCI.14	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.SCI.15	Head	**1.3 Purpose**
Eu.SCI.16	Info	This document defines the protocol stack of the standardised interface for safe communication between the Subsystem - Electronic Interlocking and EULYNX field element subsystems or adjacent systems (SCI-XX).
Eu.SCI.17	Info	This interface is designated as SCI-XX, where XX refers to the system type of the communication partner.
Eu.SCI.87	Info	This document contains the general requirements for transport, redundancy, safety and retransmission, and application layer specified for SCI-XX.
Eu.SCI.18	Info	This document is intended for the following users: • safety authorities • infrastructure managers • safety assessors • signalling system suppliers • validators
Eu.SCI.254	Info	This document is applicable for both the EU-Rail System Pillar target architecture and the EULYNX architecture. The document is delivered as a single specification fitting both the System Pillar documentation sets and the EULYNX documentation sets. EU-Rail System Pillar is the technical authority for this document.
Eu.SCI.19	Head	**1.4 Applicable standards and regulations**
Eu.SCI.90	Info	The applicable standards and regulations used in EULYNX are listed in the EULYNX Reference Document List [Eu.Doc.12].
Eu.SCI.20	Info	The references listed in the EULYNX Reference Document List [Eu.Doc.12] shall be considered where they are indicated as being applicable to SCI in the "Applies to" column of the EULYNX Reference Document List [Eu.Doc.12].

ID	Type	Requirement
Eu.SCI.21	Head	**1.5 Applicable documents**
Eu.SCI.22	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.SCI.23	Head	**1.6 Appendices**
Eu.SCI.24	Info	*- intentionally left blank -*
Eu.SCI.25	Head	**1.7 Terms and abbreviations**
Eu.SCI.26	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].
Eu.SCI.27	Head	**1.8 Variability management**
Eu.SCI.28	Info	This document describes harmonised requirements. Variability management is not applicable. The specific applicability of requirements is captured in individual interface specifications.
Eu.SCI.29	Head	**1.9 Definition of object types**
Eu.SCI.30	Info	The following definition for object types is applied in this document:
Eu.SCI.31	Info	• "Req" - This denotes a mandatory requirement.
Eu.SCI.32	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.
Eu.SCI.33	Info	• "Head" - This denotes chapter headings.
Eu.SCI.34	Head	**2 Interface definition SCI-XX**
Eu.SCI.35	Info	SCI-XX is an interface based on telegrams and consists of a protocol stack according to Figure 1. In this document, requirements for transport, redundancy, safety and retransmission, and application layer (see yellow marked layers in Figure 1 below) are specified.

ID	Type	Requirement
Eu.SCI.145	Info	Figure 1: SCI-XX protocol stack (yellow layers) 
Eu.SCI.37	Info	The SCI-XX interface application layer shall be designated as SCI-XX.PDI (PDI Process Data Interface protocol). It defines the telegrams to be exchanged between communication partners.
Eu.SCI.38	Req	The safety, retransmission and redundancy layer (safe communication according to EN 50159) in SCI-XX shall be realised with the RaSTA protocol [RaSTA].
Eu.SCI.39	Req	The transport layer in SCI-XX shall be realised as two variants. Both variants shall be supported.
Eu.SCI.147	Req	In variant 1, the transport layer shall be realised with UDP.
Eu.SCI.148	Req	In variant 2, the transport layer shall be realised with TLS over TCP. Note: There is no variant using TCP without TLS.
Eu.SCI.149	Info	Which of the two variants is used in a concrete application is defined by configuration.
Eu.SCI.40	Info	The lower layers (physical layer, data link layer and network layer) are defined by the Point of Service - Signalling, as defined in [Eu.Doc.100].
Eu.SCI.41	Head	**3 Protocol layers**
Eu.SCI.42	Head	**3.1 SCI-XX Process Data Interface protocol**

ID	Type	Requirement
Eu.SCI.43	Req	The application layer uses the Process Data Interface protocol for communication between the Subsystem - Electronic Interlocking and EULYNX field element subsystem or adjacent systems as defined in the interface specification of the respective SCI-XX.
Eu.SCI.44	Req	After a disconnection (in the lower layers of the protocol stack), Subsystem - Electronic Interlocking and EULYNX field element subsystem or adjacent system shall attempt to re-establish communication within the time $T_{max} \leq X \leq T_{max} + 20\ \%$.
Eu.SCI.249	Head	**3.1.1 Variable and bit order**
Eu.SCI.250	Req	The encoding of telegrams defined for the Process Data Interface protocol shall respect the order of content variables as defined in the respective interface specification, starting with transmission of byte 00 and counting upwards.
Eu.SCI.251	Req	The encoding of content variables shall start with the most significant bit.
Eu.SCI.45	Head	**3.2 RaSTA**
Eu.SCI.46	Req	For the application of the generic RaSTA protocol with SCI-XX, the following parameters shall be applied. For specific implementation projects, different values may be defined by national specifications. RaSTA consists of the Safety/Retransmission and Redundancy layers, the configuration parameters for each layer are defined separately. Note: These parameters have been derived from existing small scale implementations. They have to be proven by further operational experience on larger scales. Deviating values can be used for specific interfaces. Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SCI.223	Info	For variant 1 of SCI-XX (UDP), there is 1 RaSTA configuration.
Eu.SCI.224	Info	For variant 2 of SCI-XX (TLS/TCP), there are 3 RaSTA configuration profiles. a. Reduced heartbeat profile b. Fast timeout profile c. Backwards compatibility profile
Eu.SCI.225	Req	Profile c. (backwards compatibility) shall be supported.
Eu.SCI.226	Info	Support for profiles a. (reduced heartbeat) and b. (fast timeout) is optional.
Eu.SCI.150	Info	Which of the three profiles is used in a concrete application is defined by configuration.
Eu.SCI.146	Head	**3.2.1 RaSTA configuration for UDP**
Eu.SCI.247	Info	It is assumed that RaSTA parameters are related to Tmax according to the following formula: $T_{max} > 3*T_h + 2*(T_a + T_b) + T_{seq}$ plus sufficient margin. (T_a and T_b are transmission times)

ID	Type	Requirement
Eu.SCI.47	Head	**3.2.1.1 Safety/Retransmission layer configuration**
Eu.SCI.48	Head	**3.2.1.1.1 Tmax**
Eu.SCI.49	Info	T_{max} is the maximum accepted age of a message.
Eu.SCI.50	Req	T_{max} = 1800 ms
Eu.SCI.51	Head	**3.2.1.1.2 Th**
Eu.SCI.52	Info	T_h is the heartbeat interval.
Eu.SCI.53	Req	T_h = 300 ms
Eu.SCI.54	Head	**3.2.1.1.3 Safety Code**
Eu.SCI.56	Req	SafetyCode = option 2 (lower half of MD4) The initialisation value for MD4 is project specific.
Eu.SCI.57	Head	**3.2.1.1.4 Nsendmax**
Eu.SCI.58	Info	A communication partner shall not send more than $N_{sendmax}$ messages without an acknowledgement received (ReceiveBufferSize). This value is exchanged among communication partners during initialisation and can be interpreted as receive buffer minimum size.
Eu.SCI.59	Req	$N_{sendmax}$ = 20
Eu.SCI.60	Head	**3.2.1.1.5 MWA**
Eu.SCI.61	Info	A communication partner shall send an acknowledgement after receiving MWA messages (AcknowledgeWindow). MWA < $N_{sendmax}$
Eu.SCI.62	Req	MWA = 10
Eu.SCI.63	Head	**3.2.1.1.6 NmaxPaket**
Eu.SCI.64	Info	$N_{maxPaket}$ determines, how many user messages may be combined to a single Safety/Retransmission layer packet.
Eu.SCI.65	Req	$N_{maxPaket}$ = 1
Eu.SCI.66	Head	**3.2.1.1.7 NdiagWindow**
Eu.SCI.67	Info	$N_{diagWindow}$ defines the channel quality measurement window.

ID	Type	Requirement
Eu.SCI.68	Info	The value of NdiagWindow shall be defined by national specifications. The recommended default value is $N_{diagWindow}$ = 5000 Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SCI.69	Head	**3.2.1.2 Redundancy layer configuration**
Eu.SCI.70	Head	**3.2.1.2.1 Amount of physical channels**
Eu.SCI.71	Info	Amount of channels used for communication in transport layer. One channel means no redundancy.
Eu.SCI.72	Req	Amount of physical channels = 2
Eu.SCI.73	Head	**3.2.1.2.2 Check code**
Eu.SCI.75	Req	Check code = option a (no check code)
Eu.SCI.76	Head	**3.2.1.2.3 Tseq**
Eu.SCI.77	Info	T_{seq} defines the amount of time a message, received off the channels sequence, is stored (DeferTime).
Eu.SCI.78	Req	T_{seq} = 100 ms
Eu.SCI.79	Head	**3.2.1.2.4 NDiagnose**
Eu.SCI.80	Info	$N_{Diagnose}$ defines the Redundancy layers diagnostic message window.
Eu.SCI.151	Info	The value of Ndiagnose shall be defined by national specifications. The recommended default value is as follows: Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SCI.81	Info	$N_{Diagnose}$ = 200
Eu.SCI.82	Head	**3.2.1.2.5 NdeferQueueSize**
Eu.SCI.83	Info	$N_{deferQueueSize}$ defines the maximum number of entries in the deferQueue.
Eu.SCI.84	Req	$N_{deferQueueSize}$ = 4
Eu.SCI.152	Head	**3.2.2 RaSTA configuration for TLS over TCP**

ID	Type	Requirement
Eu.SCI.240	Info	It is assumed that RaSTA parameters are related to Tmax according to the following formula: $T_{max} \geq T_a + T_b + 2 \times T_h + T_{tcpre}$ T_a, $T_b = T_{cpu} + T_n$ T_{cpu}: processing time T_n: network latency T_{tcpre}: Time of retransmission on TCP layer
Eu.SCI.153	Head	**3.2.2.1 Safety/Retransmission layer configuration**
Eu.SCI.154	Head	**3.2.2.1.1 Tmax**
Eu.SCI.155	Info	A message shall be received within T_{max} after sending (MaxChannelDelay).
Eu.SCI.156	Info	Reduced heartbeat profile: T_{max} = 1800 ms
Eu.SCI.227	Info	Fast timeout profile: T_{max} = 1000 ms
Eu.SCI.241	Info	Eu.SCI.227 assumes: T_h = 300 ms, network latency T_n = 50 ms, processing time T_{cpu} = 100 ms and T_{tcpre} = 100 ms
Eu.SCI.242	Info	The value in Eu.SCI.227 will be validated and might be updated in a future release. The aim is reducing T_{max}. The effects on SMI, SDI and SSI will be considered.
Eu.SCI.228	Req	Backwards compatibility profile: T_{max} = 1800 ms
Eu.SCI.157	Head	**3.2.2.1.2 Th**
Eu.SCI.158	Info	T_h is the heartbeat interval.
Eu.SCI.159	Info	Reduced heartbeat profile: T_h = 600 ms
Eu.SCI.243	Info	Eu.SCI.159 assumes: T_{max} = 1800 ms, network latency T_n = 50 ms, processing time T_{cpu} = 100 ms and T_{tcpre} = 300 ms
Eu.SCI.244	Info	The value in Eu.SCI.159 will be validated and might be updated in a future release. The aim is processing load by reducing the heartbeat frequency. The effects on SMI, SDI and SSI will be considered.
Eu.SCI.229	Info	Fast timeout profile: T_h = 300 ms
Eu.SCI.230	Req	Backwards compatibility profile: T_h = 300 ms
Eu.SCI.160	Head	**3.2.2.1.3 Safety Code**

ID	Type	Requirement
Eu.SCI.161	Req	SafetyCode = option 2 (lower half of MD4) The initialisation value for MD4 is project specific.
Eu.SCI.162	Head	**3.2.2.1.4 Nsendmax**
Eu.SCI.163	Info	A communication partner shall not send more than $N_{sendmax}$ messages without an acknowledgement received (ReceiveBufferSize). This value is exchanged among communication partners during initialisation and can be interpreted as receive buffer minimum size.
Eu.SCI.164	Req	$N_{sendmax} = 20$
Eu.SCI.165	Head	**3.2.2.1.5 MWA**
Eu.SCI.166	Info	A communication partner shall send an acknowledgement after receiving MWA messages (AcknowledgeWindow). $MWA < N_{sendmax}$
Eu.SCI.167	Req	MWA = 10
Eu.SCI.168	Head	**3.2.2.1.6 NmaxPaket**
Eu.SCI.169	Info	$N_{maxPaket}$ determines, how many user messages may be combined to a single Safety/Retransmission layer packet.
Eu.SCI.170	Req	$N_{maxPaket} = 1$
Eu.SCI.171	Head	**3.2.2.1.7 NdiagWindow**
Eu.SCI.172	Info	$N_{diagWindow}$ defines the channel quality measurement window.
Eu.SCI.173	Info	The value of NdiagWindow shall be defined by national specifications. The recommended default value is $N_{diagWindow} = 5000$ Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SCI.174	Head	**3.2.2.2 Redundancy layer configuration**
Eu.SCI.175	Head	**3.2.2.2.1 Amount of physical channels**
Eu.SCI.176	Info	Amount of channels used for communication in transport layer. One channel means no redundancy.
Eu.SCI.177	Req	Amount of physical channels = 2
Eu.SCI.178	Head	**3.2.2.2.2 Check code**
Eu.SCI.179	Req	Check code = option a (no check code)

ID	Type	Requirement
Eu.SCI.180	Head	**3.2.2.2.3 Tseq**
Eu.SCI.181	Info	T_{seq} defines the amount of time a message, received off the channels sequence, is stored (DeferTime).
Eu.SCI.182	Info	Reduced heartbeat profile: T_{seq} = 50 ms
Eu.SCI.231	Info	Fast timeout profile: T_{seq} = 50 ms
Eu.SCI.232	Req	Backwards compatibility profile: T_{seq} = 100 ms
Eu.SCI.183	Head	**3.2.2.2.4 NDiagnose**
Eu.SCI.184	Info	$N_{Diagnose}$ defines the Redundancy layers diagnose message window.
Eu.SCI.185	Info	The value of Ndiagnose shall be defined by national specifications. The recommended default value is $N_{diagnose}$ = 200 Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SCI.186	Head	**3.2.2.2.5 NdeferQueueSize**
Eu.SCI.187	Info	$N_{deferQueueSize}$ defines the maximum number of entries in the deferQueue.
Eu.SCI.188	Req	$N_{deferQueueSize}$ = 4
Eu.SCI.85	Head	**3.3 UDP**
Eu.SCI.86	Info	*- intentionally left blank -*
Eu.SCI.189	Head	**3.4 TLS over TCP**
Eu.SCI.190	Req	The transport layer in variant 2 is a secure transport layer, consisting of two sub-layers. The security layer shall be realised with TLS. The transport layer shall be realised with TCP.
Eu.SCI.191	Head	**3.4.1 TLS**
Eu.SCI.192	Info	The parameters for the security layer are defined in the EULYNX Security specification [Eu.Doc.114] and the EULYNX Security Parameter specification [Eu.Doc.115]
Eu.SCI.193	Head	**3.4.2 TCP**
Eu.SCI.233	Info	The values of certain TCP parameters depends on the RaSTA configuration profile.

ID	Type	Requirement
Eu.SCI.194	Req	The following parameters shall be applied:
Eu.SCI.195	Head	**3.4.2.1 Nagle Algorithm (tcp_nodelay)**
Eu.SCI.196	Req	tcp_nodelay = true
Eu.SCI.197	Info	Explanation: The Nagle's algorithm is disabled to avoid buffering and combining multiple packets into one TCP-packet.
Eu.SCI.198	Head	**3.4.2.2 TCP Fast Retransmit (tcp_quickack)**
Eu.SCI.199	Req	tcp_quickack = on
Eu.SCI.200	Info	Explanation: To immediately acknowledge packets instead of waiting a bit to acknowledge multiple packets.
Eu.SCI.201	Head	**3.4.2.3 Selective Acknowledge (tcp_sack)**
Eu.SCI.202	Req	tcp_sack = enable
Eu.SCI.203	Info	Explanation: To reduce the number of retransmissions if multiple packets are lost.
Eu.SCI.204	Head	**3.4.2.4 Thin Stream-Option (tcp_thin_dupack)**
Eu.SCI.205	Req	tcp_thin_dupack = enable
Eu.SCI.206	Info	Explanation: Optimisations for interactive sessions (as opposed to streaming bulk data).
Eu.SCI.207	Head	**3.4.2.5 Linear timeouts (tcp_thin_linear_timeouts)**
Eu.SCI.208	Req	tcp_thin_linear_timeouts = false
Eu.SCI.209	Info	Explanation: Usage of exponential backoff is useful but should be well controlled to avoid too large timeouts (controlled by proper RTO-values, see Eu.SCI.212).
Eu.SCI.210	Head	**3.4.2.6 Buffers (tcp_cork)**
Eu.SCI.211	Req	tcp_cork = off
Eu.SCI.246	Info	Explanation: tcp_cork parameter delays sending out partial frames.
Eu.SCI.212	Head	**3.4.2.7 Retransmission timeout (tcp_rto_min, tcp_rto_max)**
Eu.SCI.213	Info	Reduced heartbeat profile: tcp_rto_min = 50 ms

ID	Type	Requirement
Eu.SCI.214	Info	Reduced heartbeat profile: tcp_rto_max = 400 ms
Eu.SCI.215	Info	Reduced heartbeat profile: tcp_rto_init = 200 ms
Eu.SCI.234	Info	Fast timeout profile: tcp_rto_min = 10 ms
Eu.SCI.235	Info	Fast timeout profile: tcp_rto_max = 150 ms
Eu.SCI.236	Info	Fast timeout profile: tcp_rto_init = 50 ms
Eu.SCI.237	Req	Backwards compatibility profile: tcp_rto_min = 50 ms
Eu.SCI.238	Req	Backwards compatibility profile: tcp_rto_max = 400 ms
Eu.SCI.239	Req	Backwards compatibility profile: tcp_rto_init = 200 ms
Eu.SCI.216	Info	Explanation: Retransmission Time Out (RTO) will dynamically adapt to the actual round-trip-time (network delay + processing time).
Eu.SCI.217	Head	**3.4.2.8 RTT-accuracy (tcp_timestamp)**
Eu.SCI.218	Req	tcp_timestamp = on
Eu.SCI.219	Info	Explanation: Use of TCP-timestamps according to RFC7323 for more accurate round-trip-time calculations.
Eu.SCI.220	Head	**3.4.2.9 Number of retries (tcp_retries2)**
Eu.SCI.221	Req	tcp_retries2 = 15
Eu.SCI.222	Info	Explanation: TCP-stack should keep trying to retransmit, in case of problems RaSTA will break the connection (the value 15 is the default for TCP). This value defines the time when TCP detects a connection loss based on effective Retransmission Time Out and is between tcp_retries2 * tcp_rto_min and tcp_retries2 * tcp_rto_max.