EULYNX Initiative

Europe's Rail Joint Undertaking

Interface definition and specification SMI

Document number: Eu.Doc.76
Version: 2.0 (1.A)

Contents

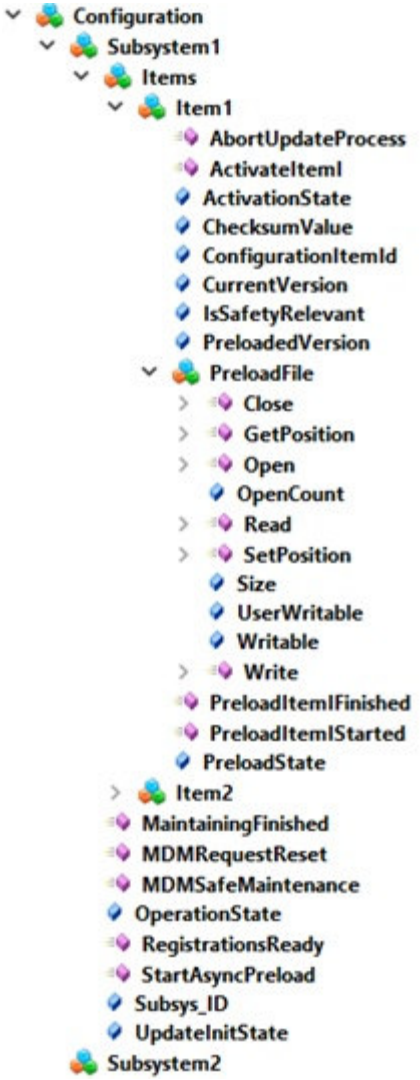
ID	Type	Requirement
Eu.SMI.5	Head	# 1 Introduction
Eu.SMI.155	Head	## 1.1 Release information
Eu.SMI.194	Info	[Eu.Doc.76] Interface definition and specification SMI CENELEC Phase: 5 Version: 2.0 (1.A) Approval date: 15.06.2023
Eu.SMI.206	Info	**Version history**
Eu.SMI.255	Info	version number: 2.0 (0.A) date: 18.05.2022 author: Andreas Strahm, Nico Huurman review: CCB changes: EUAR-508, EUAR-520, EUAR-526, EUAR-528, EUAR-529, EUAR-537
Eu.SMI.259	Info	version number: 2.0 (1.A) date: 27.06.2023 author: Nico Huurman review: TCCS+TACS Mirror Group changes: EUAR-564, EUAR-589, EUAR-594, EUAR-610, EUAR-612, EUAR-613
Eu.SMI.154	Head	## 1.2 Impressum
Eu.SMI.193	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.SMI.192	Info	Responsible for this document: EU-Rail System Pillar Transversal CCS Components domain

ID	Type	Requirement
Eu.SMI.208	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.SMI.153	Head	**1.3 Purpose**
Eu.SMI.191	Info	This document describes the Standard Maintenance Interface for the service functions Loading procedure between the Subsystem - Maintenance und Data Management (subsystem MDM) and the EULYNX field element subsystems.
Eu.SMI.190	Info	The service function Loading procedure is designed to provide both safety-critical and non-safety-critical configuration data, as well as software updates.
Eu.SMI.189	Info	This document contains general communication requirements and technical specifications (e.g. protocols and telegram definition) for the SMI (Standard Maintenance Interface) and forms the basis for manufacturer implementation.
Eu.SMI.187	Info	This document does not specify the behaviour of the respective communication partner (e.g. the system reaction in the event of a communication failure), and in particular it does not define when which telegram should be sent. This behaviour is the subject of the Maintenance and data management specification [Eu.Doc.18], the Generic interface and subsystem requirements for SMI [Eu.Doc.120] and further national requirements. Note: In future phases of the System Pillar, national specifications will be replaced by harmonised specifications.
Eu.SMI.186	Info	This document is intended for the following users: • safety authorities • infrastructure managers • safety assessors • signalling system suppliers • validators
Eu.SMI.260	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.SMI.152	Head	**1.4 Applicable standards and regulations**
Eu.SMI.184	Info	A list of applicable standards and regulations used in EULYNX is listed in the EULYNX Reference Document List [Eu.Doc.12].
Eu.SMI.205	Info	The references listed in the EULYNX Reference Document List [Eu.Doc.12] shall be considered where they are indicated as being applicable to SMI in the "Applies to" column of the EULYNX Reference Document List [Eu.Doc.12]
Eu.SMI.151	Head	**1.5 Applicable documents**

ID	Type	Requirement
Eu.SMI.183	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.SMI.150	Head	**1.6 Appendix**
Eu.SMI.175	Info	*- intentionally left blank -*
Eu.SMI.149	Head	**1.7 Terms and abbreviations**
Eu.SMI.169	Info	The terms and abbreviations are listed in the EULYNX Glossary [Eu.Doc.9].
Eu.SMI.209	Head	**1.8 Variability management**
Eu.SMI.210	Info	This document describes harmonised requirements. Variability management is not applicable.
Eu.SMI.147	Head	**1.9 Definition of object types**
Eu.SMI.162	Info	The following definition for object types is applied in this document:
Eu.SMI.161	Info	• "Req" - This denotes a mandatory requirement.
Eu.SMI.158	Info	• "Info" - This denotes additional information to help understand the specification. These objects do not specify any additional requirements.
Eu.SMI.157	Info	• "Head" - This denotes chapter headings.
Eu.SMI.4	Head	**2 Requirements**
Eu.SMI.258	Req	All references to Eu.Doc.120 refer to Generic interface and subsystem requirements for SMI version 1.0 (0.A).
Eu.SMI.141	Head	**2.1 Definition of the SMI**
Eu.SMI.145	Info	The SMI is a telegram-based interface. It is composed of the transport layer and the application layer.
Eu.SMI.144	Info	The application protocols and the application-related functional requirements associated with it are described in detail in the following chapter titled "Loading procedure".
Eu.SMI.143	Info	The transport layer of the SMI required in line with the application is specified in the chapter titled "Loading procedure".
Eu.SMI.142	Info	The lower layers (network layer, data link layer and physical layer) are defined by the PoS-Signalling [Eu.Doc.100].

ID	Type	Requirement
Eu.SMI.51	Info	The Standard Maintenance Interface (SMI) is identical for all connected systems in terms of functionality.
Eu.SMI.256	Head	**2.2 Functional requirements**
Eu.SMI.257	Info	The functional requirements for SMI-XX are described in Eu.Doc.120.
Eu.SMI.3	Head	**3 Loading procedure for Configuration data and Engineering data and for device software**
Eu.SMI.45	Head	**3.1 Overview**
Eu.SMI.212	Info	The service function Loading procedure supports the provision of engineering and configuration data and of device software to the connected systems.
Eu.SMI.44	Head	**3.2 Standard Maintenance Interface: MDM – connected system**
Eu.SMI.50	Head	**3.2.1 Communication requirements**
Eu.SMI.223	Req	If two network channels are used for the service function Loading procedure:
Eu.SMI.138	Req	• the Loading procedure shall always take place via one of the two network channels
Eu.SMI.215	Req	• when there is no reply from the MDM within 1 second, the connected system shall retry using the other network channel
Eu.SMI.136	Req	The OPC UA protocol with binary binding via OPC UA Secure Connection [OPC] via TCP shall be used for the Loading procedure.
Eu.SMI.227	Req	The notification mechanism as defined in [OPC] is used to initiate data update of the connected systems.
Eu.SMI.228	Req	OPC UA uses a strict client server model. The server shall run on the connected system. The client shall be contained in the service function Loading procedure. Note: It is recommended to integrate a COTS OPC UA client into the service function Loading procedure.
Eu.SMI.229	Req	The connection shall always be established through the service function Loading procedure.
Eu.SMI.247	Req	The service function Loading procedure may establish the connection as soon as communication on the PoS-Signalling is possible.
Eu.SMI.238	Req	If no connection is available when the connected system expects to interact with the service function Loading procedure, the OPC UA server on the connected system shall trigger the opening of the OPC UA connection by the client via reverse connect.

ID	Type	Requirement
Eu.SMI.239	Req	The establishing of the OPC UA connection shall be triggered when the connected system is entering the sub-state "Waiting for data update" within the state "Initialising".
Eu.SMI.248	Info	After the event MaintainingFinished the OPC UA connection may be either closed by the client or remains open.
Eu.SMI.230	Req	The communication between the OPC UA client and the OPC UA server shall be session-oriented. For OPC UA, a "telegram" consists of a communication session in which several OPC UA-specific messages are exchanged between the client and the server. The individual messages follow the OPC UA standard [OPC] and are not described here.
Eu.SMI.126	Req	The SubS_ID (see Eu.SAS.77) shall be used to identify the connected system in the MDM accordingly.
Eu.SMI.231	Head	**3.2.2 Information model**
Eu.SMI.241	Info	The information model, as defined in [OPC], to be used is shown in the figure below.

ID	Type	Requirement
Eu.SMI.233	Req	Information model 
Eu.SMI.244	Info	The table below contains clarifications regarding the information model in Eu.SMI.233

<table>
<tr><th>ID</th><th>Type</th><th>Requirement</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Item</th><th>Level</th><th>Meaning / Purpose</th></tr>
<tr><td>Subsystem1,
Subsystem 2</td><td>Configuration (global)</td><td>Group that contains all Configuration Items, methods and status variables used for maintaining a specific EULYNX field element Subsystem.</td></tr>
<tr><td>Items</td><td>Subsystem</td><td>Group that contains all Configuration Items (data) for a specific EULYNX field element Subsystem.</td></tr>
<tr><td>Item1, Item2</td><td>Items</td><td>The example configuration tree shows two Configuration Items (CI). There can be 1..n CIs. The attribute IsSafetyRelevant indicates whether the CI is safety relevant or not.
CIs can contain configuration and engineering data or device software.</td></tr>
<tr><td>AbortUpdateProcess</td><td>Item(n)</td><td>Event that allows the MDM to abort the currently running update of a configuration item.</td></tr>
<tr><td>ActivateItemI</td><td>Item(n)</td><td>Event used by the MDM to activate a previously transferred configuration. Activation means that it is to be installed at the EULYNX field element Subsystem.</td></tr>
<tr><td>ActivationState</td><td>Item(n)</td><td>Variable used by the EULYNX field element Subsystem to indicate to the MDM that a Configuration Item is ready for activation.
States: NotYetActivatable; ReadyForActivation; Activating; ActivationAborted</td></tr>
<tr><td>ChecksumValue</td><td>Item(n)</td><td>The value of the checksum of the Configuration Item (CI). It can be used by the EULYNX field element subsystem to check the integrity of the CI.</td></tr>
<tr><td>ConfigurationItemId</td><td>Item(n)</td><td>Unique identifier of the Configuration Item.</td></tr>
<tr><td>CurrentVersion</td><td>Item(n)</td><td>Currently applied version of the Configuration Item.
This value is set by the EULYNX field element Subsystem based on the version information read from the installed file.</td></tr>
<tr><td>IsSafetyRelevant</td><td>Item(n)</td><td>Indicates whether the Configuration Item contains safety relevant data or not.</td></tr>
</table>
</td></tr>
<tr><td>Eu.SMI.253</td><td>Info</td><td>The table below contains clarifications regarding the information model in Eu.SMI.233</td></tr>
</table>

<table>
<tr><th>ID</th><th>Type</th><th>Requirement</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Item</th><th>Level</th><th>Meaning / Purpose</th></tr>
<tr><td>PreloadedVersion</td><td>Item(n)</td><td>Version of a preloaded Configuration Item. Preloaded items can be activated immediately or at a later time if a two-step update procedure is applied.
This value is set by the EULYNX field element Subsystem based on the version information read from the preloaded file.</td></tr>
<tr><td>PreloadFile</td><td>Item(n)</td><td>File handle for writing Configuration Item data to the EULYNX field element Subsystem.
The file must contain version information.</td></tr>
<tr><td>PreloadItemIFinished</td><td>Item(n)</td><td>Event from the MDM to the EULYNX field element Subsystem indicating that the preloading of the Configuration Item has been completed.</td></tr>
<tr><td>PreloadItemIStarted</td><td>Item(n)</td><td>Event from the MDM to the EULYNX field element Subsystem indicating that the preloading of the Configuration Item has started.</td></tr>
<tr><td>PreloadState</td><td>Item(n)</td><td>Variable used by the EULYNX field element Subsystem to indicate to the MDM that a preload of the Configuration Item is possible. States: NotYetPreloadable, ReadyForPreload, Preloading, PreloadingAborted</td></tr>
<tr><td>MaintainingFinished</td><td>Subsystem</td><td>Event that notifies the EULYNX field element Subsystem that the maintenance process has been completed.</td></tr>
<tr><td>MDMRequestReset</td><td>Subsystem</td><td>Event from the MDM to the EULYNX field element Subsystem to perform a remote reset.</td></tr>
<tr><td>MDMSafeMaintenance</td><td>Subsystem</td><td>Event from the MDM to the EULYNX field element Subsystem (EfeS) to perform maintenance after the EfeS was safely released from railway operation.</td></tr>
</table>
</td></tr>
<tr><td>Eu.SMI.254</td><td>Info</td><td>The table below contains clarifications regarding the information model in Eu.SMI.233</td></tr>
</table>

<table>
<tr><th>ID</th><th>Type</th><th>Requirement</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Item</th><th>Level</th><th>Meaning / Purpose</th></tr>
<tr><td>OperationState</td><td>Subsystem</td><td>Variable that indicates the general operation state of the EULYNX field element Subsystem in the context of configurability.
States: NotMaintenance, Maintenance</td></tr>
<tr><td>RegistrationsReady</td><td>Subsystem</td><td>Event from the MDM to the EULYNX field element Subsystem (EfeS) to inform the EfeS that the registration of OPC UA status variables has been finished.</td></tr>
<tr><td>StartAsyncPreload</td><td>Subsystem</td><td>Event from the MDM to the EULYNX field element Subsystem (EfeS) to start a download that can be performed in parallel to the safe railway operation of an EfeS.</td></tr>
<tr><td>Subsys_ID</td><td>Subsystem</td><td>The unique identifier of the EULYNX field element Subsystem.</td></tr>
<tr><td>UpdateInitState</td><td>Subsystem</td><td>Variable used by the EULYNX field element Subsystem to indicate to the MDM that initialisation of PreloadState and ActivationState variables has been finished.
This is the trigger that allows the MDM to iterate over the items and update them as needed.
BooleanStates: True, False</td></tr>
</table>
</td></tr>
<tr><td>Eu.SMI.242</td><td>Req</td><td>Generic events as defined in [Eu.Doc.120] are implemented by the following mechanisms defined in [OPC], as below:</td></tr>
<tr><td>Eu.SMI.232</td><td>Req</td><td>T1in_Maintaining_finished shall be triggered by calling MaintainingFinished</td></tr>
<tr><td>Eu.SMI.234</td><td>Req</td><td>T2in_Preload_item_i_started shall be triggered by calling PreloadItemIStarted</td></tr>
<tr><td>Eu.SMI.235</td><td>Req</td><td>T3in_Preload_item_i_finished shall be triggered by calling PreloadItemIFinished</td></tr>
<tr><td>Eu.SMI.236</td><td>Req</td><td>T4in_Activating_item_i shall be triggered by calling ActivateItemI</td></tr>
<tr><td>Eu.SMI.237</td><td>Req</td><td>T6in_Update_process_aborted shall be triggered by calling AbortUpdateProcess</td></tr>
<tr><td>Eu.SMI.249</td><td>Req</td><td>T19in_Start_async_preload shall be triggered by calling StartAsyncPreload</td></tr>
<tr><td>Eu.SMI.250</td><td>Req</td><td>T30in_MDM_Request_Reset shall be triggered by calling MDMRequestReset</td></tr>
<tr><td>Eu.SMI.251</td><td>Req</td><td>T32in_Registrations_Ready shall be triggered by calling RegistrationsReady</td></tr>
</table>

ID	Type	Requirement
Eu.SMI.252	Req	T36in_MDM_Safe_Maintenance shall be triggered by calling MDMSafeMaintenance
Eu.SMI.42	Head	**3.3 Standard Maintenance Interface: MDM – Subsystem - Electronic Interlocking (SMI-EIL)**
Eu.SMI.46	Info	*- The procedure is not currently specified -*