




ERJU SYSTEM PILLAR

System Interface Description_TCCS- System Interface SMI (v3) (SERA Version)



System Interface Description_TCCS-System Interface SMI (v3) (SERA Version)

Author(s)	Karl-Albrecht Klinge , Bolz, Gert (SMO RI R&D IXL IL) , RICHTER Robert , Ghielmetti Cirillo (I-NAT-GST-CCS)
Abstract	This document describes the Standard Maintenance Interface (SMI) as required per SPPRAMSS-349 - EN 50126-1:2017 phase 5 (Architecture and apportionment of system requirements) between the Service Function Configuration (SFC) and the Building Block (BB). This document contains general communication requirements and technical specifications (e.g. protocols and application definition) for the Standard Maintenance Interface (SMI). The interactions between the respective communication partners are specified.
Config Item	System Interface Description
Document ID	TCCS Service Function Configuration _SFC_ L5/TCCS System Interface SMI_v3#723837  System Interface Description_TCCS-System Interface SMI (v3) (SERA Version)
Classification	Public
Status	In Review by System Pillar
Version	1.0
Revision	723837
Last Change Date	02.10.2025
Copyright	Brussels: Europe's Rail Joint Undertaking, 2025

© Europe's Rail Joint Undertaking, 2025

This document is drafted by and belongs to EU Rail.

EU Rail encourages the distribution and re-use of this document, the technical specifications and the information it contains. EU Rail holds several intellectual property rights, such as copyright and trade mark rights, which need to be considered when this document is used.

EU Rail authorises you to re-publish, re-use, copy and store this document without changing it, provided that you indicate its source and include the following: EU Rail trade mark, title of the document, year of publication, version of document.

EU Rail makes no representation or warranty as to the accuracy or completeness of the information contained within these documents. EU Rail shall have no liability to any party as a result of the use of the information contained herein. EU Rail will have no liability whatsoever for any indirect or consequential loss or damage, and any such liability is expressly excluded.

You may study, research, implement, adapt, improve and otherwise use the information, the content and the models in the this document for your own purposes. If you decide to publish or disclose any adapted, modified or improved version of this document, any amended implementation or derivative work, then you must indicate that you have modified this document, with a reference to the document name and the terms of use of this document. You may not use EU Rail's trade marks or name in any way that may state or suggest, directly or indirectly, that EU Rail is the author of your adaptations.


EU Rail cannot be held responsible for your product, even if you have used this document and its content. It is your responsibility to verify the quality, completeness and the accuracy of the information you use, for your own purposes.

INFO: History table is not displayed, because this document is in status **doc_contentApproval**.

RULE: History table is not displayed, in statuses: { draft doc_open doc_inprogress doc_contentApproval doc_contentDecision }

CONTACT: For more information contact Administrator

Review description

Attachments	REMINDER_ [ERJU SP] Request to review SC2.4 List of deliverables - Task 2_ Transversal Systems .pdf , Review and Approval Jens Kilian.pdf , Review and Approval Virgil Lostun.pdf
Comments	#1 Approval comment by Golebniak, Udo (SMO RI ML ADC I&C) on 2025-10-01 12:25 The current TCCS Design is focused on IP Needs. The usage in Traffic CS Environment is still to be discussed and must follow top-down design. Traffic CS has currently not reached the necessary level in the design. Target date for the Traffic CS Specification work is 2027.
Approvals	Kilian Jens : Waiting , SANGO Marc (SNCF / DIR TECHNOLOGIES INNOVATION ET PROJETS GROUPE / IR DIR RECHERCHE - PSF) : Waiting , DE NICOLA, Giuseppe : Waiting , KEFALAS, Georgios : Waiting , Julien Bois : Waiting , Oliver Knapp : Waiting , Wischy, Markus Alexander (SMO RI R&D F IL) : Waiting , HENON Frédéric : Waiting , TEKE, Emre : Waiting , Renato Rodrigues : Waiting , IOVINO, Salvatore : Waiting , Davinder Bhatia : Waiting , BITSCH Friedemann : Waiting , Roman R Treydel : Waiting , Golebniak, Udo (SMO RI ML ADC I&C) : Waiting , Mirko Blazic : Waiting , Benameur, Malik (SMO NEE RC-CH RI PLM SYS) : Waiting , MOTTOLA, Giuseppe Diodato : Waiting , Jack Schneider : Waiting , Zeeshan Z Ansar : Waiting , LOSTUN Virgil : Waiting , Patrick Konix : Waiting , NANNI Marco : Waiting , DE MARCO TELESE Giancarlo : Waiting , Tione, Roberto : Waiting , Andreeva-Moschen Emilia (HOLDING) : Waiting
Type of Approval	 Document Review

Approval description


Attachments	REMINDER_ [ERJU SP] Request to review SC2.4 List of deliverables - Task 2_ Transversal Systems .pdf , Review and Approval Jens Kilian.pdf , Review and Approval Virgil Lostun.pdf
Approvals	LOSTUN Virgil : Waiting
Type of Approval	 Document Approval

Table of Contents

1	Preamble	4
1.1	Scope and intended audience	4
1.2	Purpose	5
1.3	Glossary	5
2	Overview	5
2.1	Overall description	5
2.2	Non-functional characteristics / non-functional requirements	6
3	SMI application layer	6
3.1	Static description	6
3.1.1	Communication requirements	6
3.1.2	General OPC UA requirements	7
3.1.3	Information model	8

3.2	Dynamic description	13
3.2.1	Configuration Services	13
3.2.1.1	Loading Procedure	13
3.2.1.2	Deactivation Procedure	14
3.2.1.3	Activation Procedure	14
3.2.1.4	Confirmation Procedure	14
3.2.1.5	Backup Procedure (future; part of Cybersecurity Alignment)	14
3.2.2	Maintenance Services	14
3.2.2.1	Reset Procedure	14
3.2.2.2	SafeMaintenance Procedure	14
3.2.2.3	Factory Reset Procedure (future; part of Security Alignment)	14
3.2.3	Connection Procedures	14
3.2.3.1	SMI Connection Setup: Reverse Connection	14
3.2.3.2	SMI Connection Setup: Direct Connection	14
3.2.3.3	SMI Session Setup	14
3.2.3.4	SMI Connection / Session Termination	14
3.2.3.5	SMI Connection / Session Re-establishment	15
3.2.4	Definition of time values	15
3.2.4.1	Connection Handling	15
3.2.4.2	Update Handling	15
3.3	Interdependencies to other interface layers	16
4	Appendix	16
4.1	Input documents	16
4.2	Standards and References	16
5	Workspace for discussions, actions and issues	16
6	Scope of interface constraints	17

Table of Figures

1 Preamble

1.1 Scope and intended audience

This document defines the interface for the configuration artifact update of consumers orchestrated by the Service Function Configuration (SFC). The update procedure provides safety related and non-safety related configuration artifacts to the consumers. [SPT2TS-130542]


Intended audience includes:

- Suppliers
- Operators
- Integrators

[SPT2TS-131289]

1.2 Purpose

ToDo: Add reference to "System Definition" and "System Architecture" document.

This document describes the Standard Maintenance Interface (SMI) as required per  SPPRAMSS-349 - [EN 50126-1:2017] phase 5 (Architecture and apportionment of system requirements) between the Service Function Configuration (SFC) and the Building Block (BB).

This document contains general communication requirements and technical specifications (e.g. protocols and application definition) for the Standard Maintenance Interface (SMI). The interactions between the respective communication partners are specified.

Note: This document defines the generic System Pillar Standard Maintenance Interface (SMI). It bases on the System Pillar / EULYNX Baseline 4 Release 4 Standard Maintenance Interface (SMI_v2) applicable for EULYNX field element subsystems only.
[SPT2TS-130543]

1.3 Glossary

ToDo: Add reference to "TCCS Glossary".

2 Overview

2.1 Overall description

The SMI interface partners are the Service Function Configuration (SFC) and the configurable Building Block (BB). SMI uses the OPC UA protocol based on a client-server model. The SFC realizes the OPC UA client, while the BB realizes the OPC UA server. Basically the BB offers its capabilities to the SFC, which orchestrates the configuration management process. [SPT2TS-130544]

The SMI is a message-based interface using OPC UA (OPC Unified Architecture) protocol. It is composed of the transport layer and the application layer. [SPT2TS-130522]

The application layer handles the actual data exchange and interaction between SMI application peer nodes. It defines the information model, services, data types, and security like authorization to enable interoperability. The application layer communicates over a secure channel established by the transport layer. The application-related functional requirements are described in this document. [SPT2TS-130523]

The transport layer of the SMI is responsible for the secure and reliable transmission of messages between clients and servers. It includes mechanisms such as the OPC UA Secure Channel, which provides encryption, message signatures, and certificates for application authentication. The transport-related functional requirements are described in this document [SPT2TS-130520]

The lower layers (network layer, data link layer and physical layer) are defined by the PoS-Signalling [Eu.Doc.100].

ToDo: Add reference to "PoS-Signalling [Eu.Doc.100]" [SPT2TS-130521]

The Standard Maintenance Interface (SMI) is identical for all connected CCS/TMS systems in terms of functionality.
[SPT2TS-130519]

2.2 Non-functional characteristics / non-functional requirements

ToDo: Add references to further applicable work items from PRAMS, etc.

TCCS System L4:

■ SPT2TS-127949 - **Non-functional system requirements** [SPT2TS-130539]

System Pillar Cybersecurity:

- SPPRAMSS-2785: SP-SEC-CommSpec - OPC UA Secure Communication Requirements
- SPPRAMSS-1563: SP-SEC-CompSpec - Software Update Requirements
- SPPRAMSS-1553: SP-SEC-CompSpec - Secure Component Configuration Requirements
- SPPRAMSS-2465: SP-SEC-CompSpec - Device Software Requirements
- SPPRAMSS-1495: SP-SEC-ServSpec - Shared Cybersecurity Services Requirements [SPT2TS-130540]

System Pillar Transversal CCS design decisions:

- **TCCS SD3 Logical Architecture Solution Variants** [SPT2TS-130538]

3 SMI application layer

The Standard Maintenance Interface (SMI) enables the transfer of safety related and non-safety related configuration artifacts between the Service Function Configuration (SFC) and a Building Block (BB).

3.1 Static description

The static description specifies the foundational, immutable elements that define the interface capabilities and characteristics. This includes the following aspects: Information model, services, data type specification, namespace conventions, security mechanisms. These elements form the basis upon which the dynamic aspects of the interface are built.

3.1.1 Communication requirements

SPT2TS-130558 - The OPC UA endpoint shall use OPC UA Secure Conversation with binary encoding over TCP (UA-TCP UA-SC UA-Binary) ■ **SPT2TS-130528** - [OPC UA-10000-6] .

SPT2TS-130564 - The OPC UA endpoint shall use SignAndEncrypt as security mode.

SPT2TS-130559 - The OPC UA endpoint shall use mutual authentication via certificates.

SPT2TS-130560 - The OPC UA endpoint shall enforce the permissions attached to each node of the OPC-UA model.

SPT2TS-130561 - The OPC UA endpoint shall support the Security Policy ECC-nistP256.

Note: This Security Policy is defined in Amendment 4: ECC for UACore 1.04.

SPT2TS-130562 - The OPC UA endpoint shall support the Security Policy ECC-brainpoolP256r1

Note: This Security Policy is defined in Amendment 4: ECC for UACore 1.04.

SPT2TS-130563 - The OPC UA endpoint may support the Security Policy SecurityPolicy [B] – Basic256Sha256

Note: The preferred Security Policies are the ones using Elliptic Curve Cryptography (ECC). Support for RSA may be required for backwards compatibility implementations which do not support ECC yet. RSA will be removed in a future version of the System Pillar Cybersecurity Specifications.

SPT2TS-129902 - The OPC UA endpoint shall use the client-server model. The Service Function Configuration (SFC) shall realize the OPC UA client. The Building Block shall realize the OPC UA server.

SPT2TS-129883 - The communication between the OPC UA client and the OPC UA server shall be session-oriented.

The individual messages follow the OPC UA standard [OPC] and are not described here.


SPT2TS-130529 - If no connection is available when the Service Function Configuration (SFC) expects to interact with the Building Block (BB), the SFC shall establish the OPC UA connection.

SPT2TS-129891 - If no connection is available when the Building Block (BB) expects to interact with the Service Function Configuration (SFC), the BB shall trigger the SFC via reverse connect to establish the OPC UA connection.

SPT2TS-130530 - After the Service Function Configuration (SFC) performed all planned SMI maintenance activities (MaintainingFinished), the SFC shall terminate the OPC UA connection.

SPT2TS-130533 - If an active OPC UA connection is lost and there are pending SMI maintenance activities, the Service Function Configuration (SFC) shall re-establish the OPC UA connection.

Note: This handling applies regardless of which OPC UA endpoint requested the connection establishment.

SPT2TS-129888 - In case the Service Function Configuration (SFC) does not start with the establishment of the OPC UA connection as a reaction to the reverse connect within  [SPT2TS-131332](#), the Building Block (BB) shall resend the reverse connect.

Note: If an alternative endpoint of the Service Function Configuration (SFC) is configured, the BB shall use this endpoint for the retry.

SPT2TS-129911 - If two network channels (primary, secondary) are used for the SMI maintenance activities, the maintenance activities shall always use the primary network channel, if available.

SPT2TS-130535 - If two network channels (primary, secondary) are used for the SMI maintenance activities and the primary network channel is not available, the maintenance activities shall use the secondary network channel.

SPT2TS-130536 - If two network channels (primary, secondary) are used for the SMI maintenance activities and the primary network channel is available again, the maintenance activities shall use the primary network channel for upcoming SMI maintenance activities.

Note: Constant toggling between network channels needs to be prevented.

SPT2TS-129882 - The bbId shall be used to uniquely identify the Building Block (BB).

SPT2TS-130578 - The bbCId shall be used to uniquely identify the Building Block Configuration (BBC) within a specific Building Block (BB).

SPT2TS-130579 - The bbCId together with attribute "CurrentVersion" (bbcVersion) denotes a specific incarnation of a Building Block Configuration (BBC).

SPT2TS-129881 - The target address(es) and the corresponding communication ports of the OPC UA client used for initiating the reverse connect shall be configurable at the Building Block (BB).

Note: If two network channels are used for the Service Function Configuration (SFC), two target addresses need to be configurable.

Note: In order to ensure compatibility and interoperability it is recommended to use the standard TCP port number (4840) for the OPC UA communication.

SPT2TS-129880 - The allowed communication ports of the OPC UA server for establishment of the OPC UA connection by the Service Function Configuration (SFC) shall be configurable at the Building Block (BB).

Note: In order to ensure compatibility and interoperability it is recommended to use the standard TCP port number (4840) for the OPC UA communication.

3.1.2 General OPC UA requirements

The SMI interface utilizes OPC UA as follows:

- The SMI OPC UA information model is structured using OPC UA Object-Nodes to represent the data and functionality.
- The SMI OPC UA information model remains static at runtime.
- Stateful data is exposed through OPC UA Variable-Nodes.

- The Service Function Configuration (SFC) is able to read from and subscribe to these OPC UA Variable-Nodes, but is not permitted to write to them.
- The Service Function Configuration (SFC) utilizes OPC UA method calls to invoke specific functionality (e.g., triggering actions or computations) on the Building Block (BB).

SPT2TS-130589 - The OPC UA Information model provided with this specification (SMI OPC UA Information Model) shall be used by the SMI communication partners.

Note: The specified SMI information model can be parameterized for specific configurations, while still fulfilling this specification.

SPT2TS-130740 - The existing OPC UA StatusCodes [OPC UA-Call Service Result Codes] shall be reused for application specific error information after completion of an OPC UA method call.

Note: To eliminate any vagueness, the OPC UA server should include the application specific description in the DiagnosticInfo.

SPT2TS-130742 - The OPC UA client shall not be enabled for the writing of variables on the OPC UA server..

SPT2TS-129878 - OPC UA node IDs of system parts in the OPC UA server of the connected system shall remain unchanged after a reset of the connected system or of the OPC UA server, unless an OPC UA Node ID has been explicitly changed during a configuration update.

SPT2TS-131336 - The OPC UA server in the connected system shall implement the "Embedded 2017 UA Server Profile".

The binary protocol defined in the "Standard 2017 UA Server Profile" is used for communication.

SPT2TS-129884 - The following facets shall be implemented in addition:

- Reverse Connect Server Facet / Reverse Connect Client Facet
- Method Server Facet / Method Client Facet
- File Access Server Facet / File Access Client Facet

SPT2TS-130565 - The OPC UA server on the connected system shall respect the security permissions. The following security permissions are used:

- eu.rail.smi.configuration-read -- abbr.: R
- eu.rail.smi.configuration-distribute -- abbr.: D
- eu.rail.smi.configuration-activate -- abbr.: A
- eu.rail.smi.component-reset -- abbr.: RT

Note: Please refer to ServiceFunctionConfiguration_SPT2TS-129933 for the detailed definition of the OPC UA permissions.

3.1.3 Information model

The OPC UA information model is the foundation that defines the data, functionality, and semantics exposed by OPC UA servers. It encompasses: data representation, functional representation, namespace and versioning, metadata and semantics, extensibility and interoperability.

SPT2TS-131337 - Namespace and model versioning:

- In general the model version shall consist of 3 levels M.m.c, expressing Major, minor, compatible changes.
- Major version changes indicate breaking, backward-incompatible changes to the information model
- Minor version changes represent smaller, backward compatible updates like new features or functionality.
- Compatible version changes represent minimal, backward compatible updates like minor improvements.
- Each namespaceURI shall be unique within the OPC UA server.
- Each namespace is identified by a unique namespaceURI that includes the version information M.m.

- The version information shall be appended to the namespaceURI.
- The build-in OPC UA namespace version attribute shall be set in accordance with the version information M.m.c
- An OPC UA client shall use the namespaceURI to uniquely identify a namespace

SPT2TS-130759 -

The following pattern should be used for the namespaceURI:

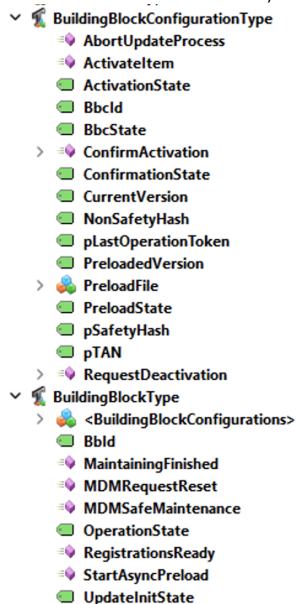
`http://[organisation]/[interface]/[interface-specific]/[version]`

where [version] should use a major.minor numbering schema

Example:

`http://rail-research.europe.eu/SMI/GEN/1.0 -- SMI generic`

The information model, as defined in [OPC] , to be used is shown in the figure below.



ToDo Incorporate EULYNX BL4R4 Eu.Doc.76 SMI information model (SMI_v2) changes

ToDo Align SMI OPC UA information model with table below (SPT2TS-129908).

ToDo Add reference to SMI OPC UA information model (xml) [SPT2TS-130582]

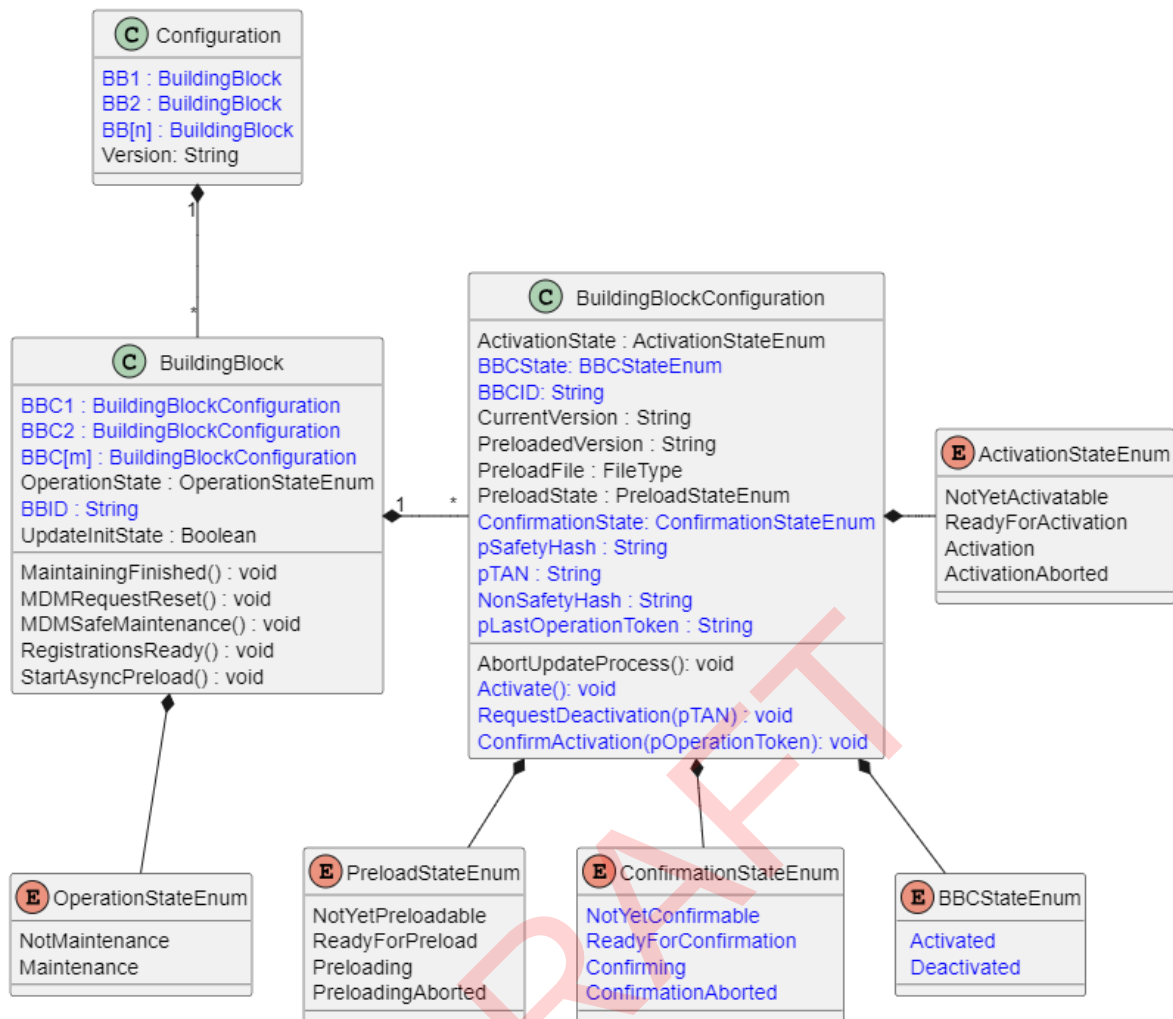
SPT2TS-129908 - The table below contains clarifications regarding the information model in SPT2TS-130582.

Name	Node Class	Parent	Additional Information	Description	Permission (R, D, A, RT)
BB1 .. BBn	Object	Configuration (global)		Contains all Building Block Configurations (BBCs), methods and status variables used for maintaining a specific Building Block.	R, D, A, RT
BBC1 .. BBCm	Object	BB (n)		Contains all methods and status variables used for maintaining a specific Building Block Configuration.	R, D, A, -
Activation State	Variable	BBC (m)	DataType: Enumeration Values: NotYetActivatable	Indicates the activation state of Building Block Configuration m	R, -, A, -

Name	Node Class	Parent	Additional Information	Description	Permission (R, D, A, RT)
			ReadyForActivation, Activating, ActivationAborted		
BBCState	Variable	BBC (m)	DataType: Enumeration Values: Activated, Deactivated	The state of the BBC, whether it is activated or deactivated.	R, D, A, -
BBCID	Variable	BBC (m)	DataType: String	<p>The unique identifier of the Building Block Configuration within the Building Block.</p> <p>The BBCID together with "CurrentVersion" denotes a specific incarnation of a Building Block Configuration.</p> <p>Remark: The BBCID is allocated and maintained by the supplier (e.g. firmware) or integrator (e.g. configuration). The BBCID is unique within a specific Building Block (BBID).</p>	R, D, A, -
CurrentVersion	Variable	BBC (m)	DataType: String	<p>Currently applied version of the Building Block Configuration.</p> <p>This value is set by the BB based on the version information read from the installed file.</p>	R, D, A, -
PreloadedVersion	Variable	BBC (m)	DataType: String	<p>Version of a preloaded Building Block Configuration. Preloaded BBCs can be activated immediately or at a later time if a two-step update procedure is applied. This value is set by the Building Block based on the version information read from the preloaded file.</p>	R, D, -, -
PreloadFile	Object	BBC (m)	DataType: FileType (OPC UA)	The preload file for Building Block Configuration m.	R, D, -, -
PreloadState	Variable	BBC (m)	DataType: Enumeration Values: NotYetPreloadable, ReadyForPreload, Preloading, PreloadingAborted	Indicates the preload state of Building Block Configuration m.	R, D, -, -

Name	Node Class	Parent	Additional Information	Description	Permission (R, D, A, RT)
ConfirmationState	Variable	BBC (m)	DataType: Enumeration Values: NotYetConfirmable, ReadyForConfirmation, Confirming, ConfirmationAborted	The confirmation state of a BBC, whether it is confirmed, not confirmed or currently confirming.	R, -, A, -
pSafetyHash	Variable	BBC (n)	DataType: String	The protected safety hash of the Building Block Configuration post installation. The safety hash is protected with the TAN.	R, -, A, -
pTAN	Variable	BBC (n)	DataType: String	Building Block generates a random value TAN and combines it with the Building Block secret to a pTAN.	R, -, A, -
NonSafetyHash	Variable	BBC (n)	DataType: String	The unprotected non safety-related hash Building Block Configuration post installation.	R, -, A, -
pLastOperationToken	Variable	BBC (m)	DataType: String	The protected value of the old OperationToken to proof that the deactivation of the incompatible Building Block Configurations has been done.	R, -, A, -
AbortUpdateProcesses	Method	BBC (m)	Inputs: no input arguments Outputs: no output arguments	Abort the currently running update of Building Block Configuration m.	-, D, A, -
Activate	Method	BBC (m)	Inputs: no input arguments Outputs: no output arguments	Activate the previously transferred building block configuration item m.	-, -, A, -
RequestDeactivation	Method	BBC (m)	Inputs: pTAN Outputs: no output arguments	Request to deactivate incompatible Building Block Configurations. This could potentially mean going out of operation for a Building Block. For non safety-related items the pTAN is empty.	-, -, A, -
ConfirmActivation	Method	BBC (m)	Inputs: pOperationToken Outputs: no output arguments	Confirm BBC activation. For non safety-related BBCs the pOperationToken is empty.	-, D, A, -
MaintainingFinished	Method	BB (n)	Inputs: no input arguments Outputs: no output arguments	Indicates that the maintenance process has been completed.	-, D, A, -
MDMRequestReset	Method	BB (n)	Inputs: no input arguments Outputs: no output arguments	Request a remote reset of the Building Block.	-, -, -, RT

Name	Node Class	Parent	Additional Information	Description	Permission (R, D, A, RT)
MDMSafeMaintenance	Method	BB (n)	Inputs: no input arguments Outputs: no output arguments	Perform maintenance after the Building Block was safely released from railway operation.	-, D, A, -
OperationState	Variable	BB (n)	DataType: Enumeration Values: NotMaintenance, Maintenance	Indicates the general operation state of the Building Block in the context of configurability.	R, D, A, -
RegistrationsReady	Method	BB (n)	Inputs: no input arguments Outputs: no output arguments	Inform the Building Block that the registration of OPC UA status variables has been finished.	-, D, A, RT
StartAsyncPreload	Method	BB (n)	Inputs: no input arguments Outputs: no output arguments	Start a download that can be performed in parallel to the safe railway operation of an Building Block.	-, D, -, -
BBID	Variable	BB (n)	DataType: String	<p>The unique identifier of the Building Block.</p> <p>Remark: The BBID is allocated and maintained by the integrator and represents an unique identifier of a BB (that could be a technical system or subsystem identifier). The BBID is used for device binding during safety attestation.</p>	R, D, A, -
UpdateInitState	Variable	BB (n)	DataType: Boolean	<p>Indicates that initialization of PreloadState and ActivationState variables has been finished.</p> <p>This is the trigger that allows the MDM to iterate over the BBCs and update them as needed.</p>	R, D, A, -



ToDo Align SMI OPC UA information model overview with table (SPT2TS-129908). [SPT2TS-130588]

3.2 Dynamic description

The dynamic description covers aspects of the interface that can change or vary as the interface is used over time. It focuses runtime behavior, configuration and settings, state changes, error handling, performance and scalability.

The dynamic description complements the static description of the interface's fundamental definitions and capabilities.

3.2.1 Configuration Services

3.2.1.1 Loading Procedure

The Loading Procedure shall be used between the SFC and the BB for cached loading of configuration data to the BB in the following situations:

- due to an administrative change of the BB configuration data in the SFC e.g. version switch;
- due to a restart of a new BB without or outdated configuration data;
- due to a request from a BB to check the validity of the current configuration data.

This procedure covers the information flows of the interface between the SFC and the BB as shown in the sequence SPT2TS-130597_Loading.

3.2.1.2 Deactivation Procedure

- => Deactivate Current Configuration & Withdraw OP-Token
- => Reference to SRS_SFC-BB SPT2TS-130592_Deactivation

3.2.1.3 Activation Procedure

- => Install New Configuration & Prepare Data Correctness Parameter
- => Reference to SRS_SFC-BB SPT2TS-130593_Activation

3.2.1.4 Confirmation Procedure

- => Check Data Correctness & Release OP-Token
- => Reference to SRS_SFC-BB SPT2TS-130594_Confirmation

3.2.1.5 Backup Procedure (future; part of Cybersecurity Alignment)

- => Parameter backup / restore
- => Reference to SRS_SFC-BB (TBD)

3.2.2 Maintenance Services

3.2.2.1 Reset Procedure

- => Request the BB to process a restart

3.2.2.2 SafeMaintenance Procedure

- => Inform the BB about pending maintenance actions

3.2.2.3 Factory Reset Procedure (future; part of Security Alignment)

- => Request the BB the process a factory reset due to decommissioning

3.2.3 Connection Procedures

3.2.3.1 SMI Connection Setup: Reverse Connection

- => BB triggered OPC UA Connection Establishment via ReverseHello

3.2.3.2 SMI Connection Setup: Direct Connection

- => SFC triggered OPC UA Connection Establishment

3.2.3.3 SMI Session Setup

- => OPC UA Session Establishment

3.2.3.4 SMI Connection / Session Termination

- => Termination of the OPC UA Connection / Session

3.2.3.5 SMI Connection / Session Re-establishment

=> Re-establishment of a terminated OPC UA Connection / Session

3.2.4 Definition of time values

3.2.4.1 Connection Handling

Con_tmax_ReverseConnection_Response: The configured value shall be the time the Building Block (BB) shall wait for a reaction of the Service Function Maintenance (SFC) ("Hello Message") after issuing a reverse connection ("Reverse Hello Message") before retrying.

DefinedBy: BB

Unit: seconds

Range: 1 - 300

Default: 1 [SPT2TS-131332]

Con_tmax_Response_SFC: The configured value shall be used to determine inactivity of the Service Function Configuration (SFC) on an established SMI connection. The SFC is considered as inactive if it does not call any SMI method during Con_tmax_Response_MDM after its last method call has been executed and returned.

The time value shall be configured in accordance with:

DefinedBy: BB

Unit: seconds

Range: 5 - 300

Default: 10 [SPT2TS-130498]

Con_tmax_SMI_Connection: The configured value shall be the time limit for trying to establish a SMI connection via reverse connection procedure. If the limit is exceeded the Building Block (BB) shall stop retrying to establish the SMI connection and continue with its current workflow.

A value smaller or equal to Con_tmax_ReverseConnection_Response implies that the Building Block (BB) only tries to connect once and does not retry at all.

DefinedBy: BB

Unit: seconds

Range: 1 - 3600

Default: 20 [SPT2TS-131333]

3.2.4.2 Update Handling

Con_tmax_DataInstallation: The configured value shall be the time limit for the activation of a Building Block Configuration (BBC). If exceeded, the Service Function Maintenance (SFC) retries or aborts the activation of the BBC.

DefinedBy: SFC

Unit: seconds

Range: 1 - 600

Default: 60 [SPT2TS-130501]

Con_tmax_DataTransmission: The configured value shall be the time limit for the transmission of a Building Block Configuration (BBC). If exceeded, the Service Function Configuration (SFC) retries or aborts the transmission of the BBC. The measured time frame starts with the call of PreloadFile.Open and ends with the call of PreloadFile.Close.

DefinedBy: SFC

Unit: seconds

Range: 60 - 3600

Default: 300 [SPT2TS-130502]

3.3 Interdependencies to other interface layers

***ToDo:** Analysis of dependencies between levels like time-out values among OSI layers, disconnection detection and reconnection.*

4 Appendix

4.1 Input documents

4.2 Standards and References

[OPC]

OPC Unified Architecture Specification (IEC/TR 62541)

- Part 1: Overview and concepts
- Part 2: Security Model
- Part 3: Address Space Model
- Part 4: Services
- Part 5: Information Model
- Part 6: Mappings
- Part 7: Profiles
- Part 8: Data Access

[OPC UA-10000-6]

OPC 10000-6: UA Part 6: Mappings

[OPC UA-Call Service Result Codes]

OPC 10000-4: UA Part 4: Services - 5.12.2.4 StatusCodes

5 Workspace for discussions, actions and issues

- The statements marked with **ToDo** will be incorporated as part of the document update planned for the next system pillar remit phase (2025/2026).

- Continue system pillar cybersecurity alignment on SSI-MNT and backup services.
- Incorporate and link with L4 results

6 Scope of interface constraints

Intentionally left blank.

DRAFT