RCA

Reference CCS Architecture

An initiative facilitated by the ERTMS Users Group and the EULYNX consortium

RCA System Architecture

Preliminary issue

Document id: RCA.Doc.35

REVISION HISTORY

Version	Date	Superseded documents/description/details	Change Request No
0.0.7	3.12.2019	Initial snapshot publication of this document	
0.1.2	27.6.2020	Improved descriptions of systems, interfaces and actors. Updated diagrams	
0.1.3	10.09.2020	Integrated review feedback from RCA Core Group	
0.2 (0.A)	11.09.2020	Document approved by RCA Core Group	

TABLE OF CONTENTS

1. Introduction 5
1.1. Release information 5
1.2. Imprint 5
1.3. Methodology conformance declaration 5
1.4. Purpose of the document 5
1.5. References 6
2. System definition (CENELEC Phase 2) 7
2.1. System context 7
2.2. Descriptions of actors 8
2.2.1. Adjacent IO systems 8
2.2.2. Adjacent Signalling System 8
2.2.3. Asset Manager 8
2.2.4. Level Crossing protection facility 8
2.2.5. Mobile Object 8
2.2.6. Monitoring System 8
2.2.7. Planning System 9
2.2.8. Point Machine 9
2.2.9. Railway Operator 9
2.2.10. Railway Vehicle 9
2.2.11. Sys Admin 9
2.2.12. Trackside Person 9
2.2.13. Train Driver 9
2.3. UseCases 9
3. Subsystem architecture (CENELEC Phase 5) 10
3.1. Layering of Logical Architecture 10
3.2. Authentication/Authorisation Interfaces 12
3.3. Configuration Management Interfaces 13
3.4. Diagnostic Monitoring Interfaces 14
3.5. Functional Interfaces 15
3.6. Workbench Interfaces 16
3.7. RCA Subsystems 16
3.7.1. SubSys MT 17
3.7.2. SubSys OA 17
3.7.3. SubSys SL 17
3.7.4. SubSys SM 17
3.7.5. SubSys VS 18
3.7.6. SubSys PE 18
3.7.7. SubSys AE 18
3.7.8. SubSys MOT 19
3.7.9. SubSys FOT 19
3.7.10. SubSys MOL 19
3.7.11. SubSys PSL 19
3.7.12. SubSys VL 20
3.7.13. SubSys AT 20
3.7.14. SubSys AV 20
3.7.15. SubSys WB 20
3.7.16. SubSys EDP 21
3.7.17. SubSys Topo4 21
3.7.18. SubSys DCM 21

3.7.19. SubSys DM 21
3.7.20. SubSys IAM 22
3.7.21. SubSys TDS 22
3.7.22. SubSys LS 22
3.7.23. SubSys P 22
3.7.24. SubSys LC 22
3.7.25. SubSys IO 22
3.8. Interfaces 22
3.8.1. ETCS SS-026 22
3.8.2. SCI-MD 23
3.8.3. SCI-AO 23
3.8.4. SCI-CMD 23
3.8.5. SCI-OP 24
3.8.6. SCI-AD 24
3.8.7. SHI-SL 24
3.8.8. AoE SS-126 25
3.8.9. SCI-VL 25
3.8.10. AoE SS-130 25
3.8.11. SHI-PE 25
3.8.12. SHI-MOT 25
3.8.13. ETCS SS-039 25
3.8.14. SHI-IAM 26
3.8.15. SCI_R1 26
3.8.16. SWI-PE 26
3.8.17. SWI-TOPO4 26
3.8.18. SWI-EDP 26
3.8.19. SWI-DCM 26
3.8.20. SWI-IAM 26
3.8.21. SWI-DM 26
3.8.22. SDI 27
3.8.23. SMI 27
3.8.24. SAI 27
3.8.25. AoE SS-132 27
3.8.26. SHI-SM 27
3.8.27. SCI-TDS 27
3.8.28. SCI-P 27
3.8.29. SCI-LC 27
3.8.30. SCI-IO 28
3.8.31. SCI-LS 28

1. INTRODUCTION

1.1. Release information

Basic document information:

RCA.Doc.35

RCA System Architecture

Cenelec Phase: 2, 4, 5

Version: 0.2 (0.A)

RCA Baseline set: 0

Approval date: 11 Sep 2020

Disclaimer:

This issue is a preliminary version of this document. The content of this document reflects the current ongoing specification work of RCA. Formal requirements management and change management will be introduced in future iterations. The content may be unfinished, will likely contain errors and can be changed without prior notice. Unfinished work is be declared by using the ToDo label in this document.

1.2. Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback

For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu.

1.3. Methodology conformance declaration

This RCA interface specification shall conform to the EULYNX Modelling Standard Baseline (https://eulynx.eu/index.php/documents/documents-overview/baseline-set-3).

1.4. Purpose of the document

The RCA system architecture specification (this document) describes the overall logical architecture. It provides system context definition, system use cases and subsystem architecture (i.e. the partitioning of the whole system into smaller subsystems).

Together with the domain knowledge and glossary, this document provides the specification of the RCA system. The RCA system architecture is the formal way of describing the earlier published RCA architecture poster (refer to RCA.Doc.40).

1.5. References

The last delivered version of all RCA documents are available on Basecamp (https://3.basecamp.com/4168621/buckets/10801981/vaults/1592502777).

Every release includes a document plan with an overview of all available documents and their current version. Refer to RCA.Doc.6

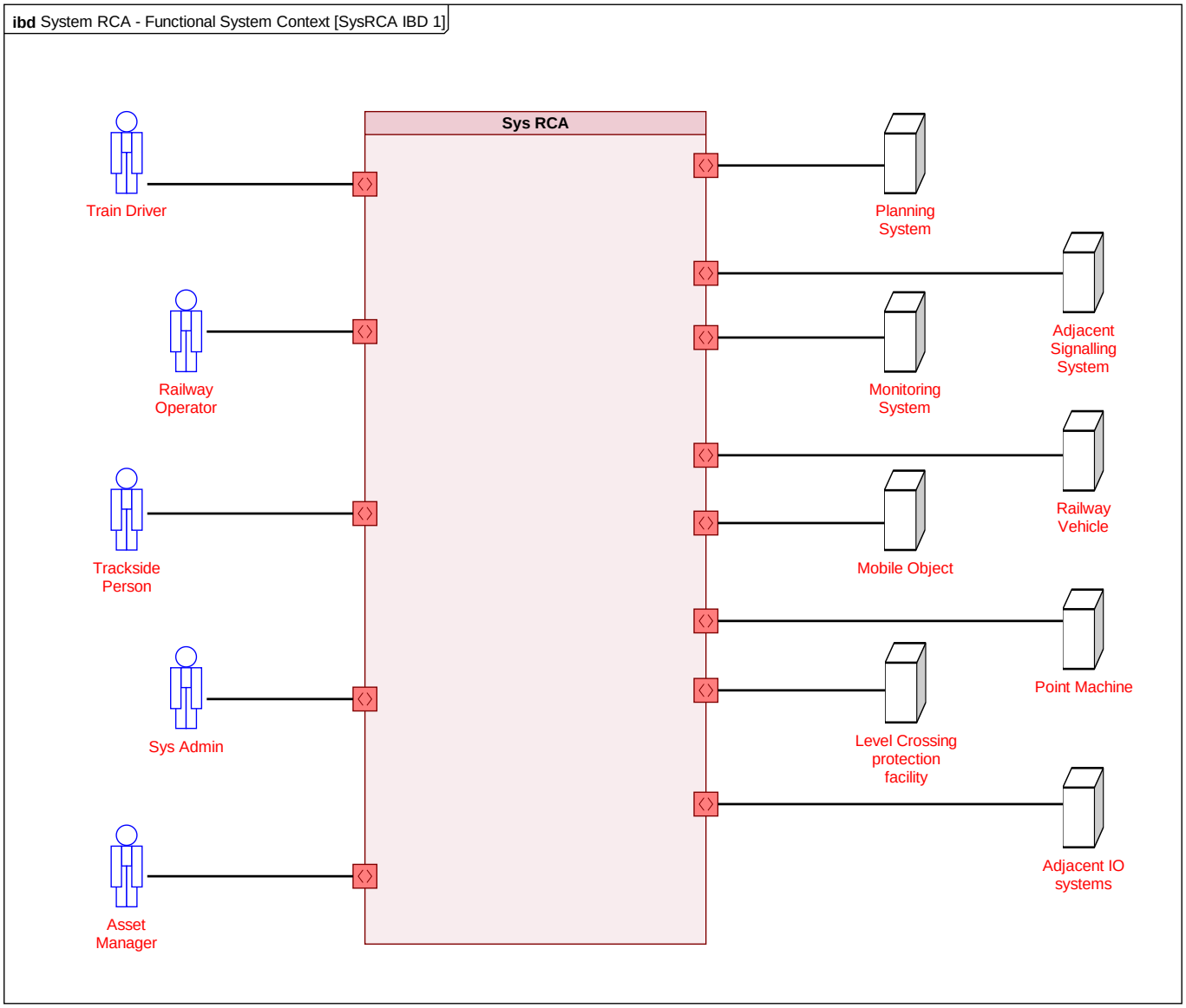
Other referenced documents:

- CCS TSI ATO over ETCS SUBSET-126
- CCS TSI ATO over ETCS SUBSET-130
- CCS TSI ATO over ETCS SUBSET-131
- CCS TSI ATO over ETCS SUBSET-132
- CCS TSI ETCS SUBSET-026
- CCS TSI ETCS SUBSET-039
- CCS TSI ETCS SUBSET-098
- CCS TSI ETCS SUBSET-119
- CCS TSI ETCS SUBSET-129
- EULYNX Eu.Doc.36
- EULYNX Eu.Doc.43
- EULYNX Eu.Doc.45
- EULYNX Eu.Doc.9
- EULYNX Eu.Doc.32
- EULYNX Eu.Doc.33
- EULYNX Eu.Doc.38
- EULYNX Eu.Doc.39
- EULYNX Eu.Doc.40
- EULYNX Eu.Doc.41
- EULYNX Eu.Doc.44
- EULYNX Eu.Doc.46

2. SYSTEM DEFINITION (CENELEC PHASE 2)

2.1. System context

Description: Sys RCA is a railway Command Control and Signalling system (CCS). Sys RCA contains all functions to safely and efficiently control movements and restrictions on the tracks. Sys RCA is connected to other systems and human actors over external interfaces. Sys RCA consists of subsystems, described in System RCA SR - Layering of Logical Architecture [SysRCA SR IBD 1].



Description: System RCA - Functional System Context [SysRCA IBD 1] shows Sys RCA in its context. The diagram shows all actors interacting with Sys RCA. The diagram shows a black box view of Sys RCA.

2.2. Descriptions of actors

This section contains the description of all actors interacting with Sys RCA and the subsystems of Sys RCA. The actors in this section are external to Sys RCA and therefore not part of the system. Actors may be systems or human beings.

2.2.1. Adjacent IO systems

Description: The Adjacent IO systems is interfaced by the physical Input Channels and/or Output Channels of the SubSys IO. Via the Output Channels, the Adjacent IO systems receives (binary On/Off) status information from the Adjacent Signalling System for evaluation and triggering of actions; via the Input Channels, the Adjacent IO systems sends (binary On/Off) status information to the Adjacent Signalling System for the same intended purpose.

Examples of Adjacent IO systems are a key lock, a departure signal or a moveable bridge. Refer to EULYNX_Eu.Doc.9.

2.2.2. Adjacent Signalling System

Description: Adjacent Signalling System can be an RCA compliant system or an existing Interlocking system.

2.2.3. Asset Manager

Description: The Asset Manager provides all relevant rail infrastructure data and manages this data. Especially the management of infrastructure data may include processes to ensure correct data preparation and data validation such that it is suitable for usage within SubSys EDP.

2.2.4. Level Crossing protection facility

Description: All equipment at a Level Crossing protection facility protecting vehicles and persons crossing the tracks (e.g. half/full barriers, obstacle detectors and road signals). Refer to EULYNX_Eu.Doc.9.

2.2.5. Mobile Object

Description: An object that is reporting to RCA system but is not able to be controlled directly by RCA, e.g. Construction Equipment, wagon, etc.

2.2.6. Monitoring System

Description: A system that monitors the operation and performance of all kind of railway infrastructure (e.g. Field Elements, Railway Vehicles, etc.), Devices, IT-systems (Software/Hardware), and communication infrastructure. This system detects errors and degradation of operational functions by analysing malfunctions of monitoring and diagnostic data, and initiates corrective actions.

2.2.7. Planning System

Description: Planning System is the planning system for the traffic management. It represents the functionality for preparing and optimising the long-term and short-term production plan. Out of this production plan the Planning System produces Operational Plans so that RCA is able to command and control the traffic operations according the production plan.

2.2.8. Point Machine

Description: The Point Machine is an apparatus for moving and securing point blades from a source of power, usually electric. The Point Machine is a safety relevant signalling system, ensuring safe passage of Railway Vehicles over moveable elements at Points, crossings and derailers. Refer to EULYNX_Eu.Doc.9.

2.2.9. Railway Operator

Description: The Railway Operator manages, directs and facilitates the movement of trains over an assigned area. This may be part, or all, of an RCA Area of Control.

2.2.10. Railway Vehicle

Description: A Railway Vehicle can be a train unit, consist or a vehicle.

2.2.11. Sys Admin

Description: Full name: System Administrator. Sys Admin is responsible for the technical operation and maintenance of the RCA systems, including Software, Hardware and communication systems. Provides and uses data with respect to the status of Software, Hardware and communications systems.

2.2.12. Trackside Person

Description: Trackside Person is a person working on the tracks for the construction or maintenance of the trackside infrastructure.

2.2.13. Train Driver

Description: A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible and safe manner.

Source: Directive 2007/59/EC of the European Parliament and of the Council

2.3. UseCases

The UseCases will be defined in later deliveries.

3. SUBSYSTEM ARCHITECTURE (CENELEC PHASE 5)

The logical architecture provides a white box view of Sys RCA. It defines the internal structure of Sys RCA. Note that the current version of this interface specification covers ATO GoA 2, but it is not yet complete with respect to ATO GoA 3/4.

3.1. Layering of Logical Architecture

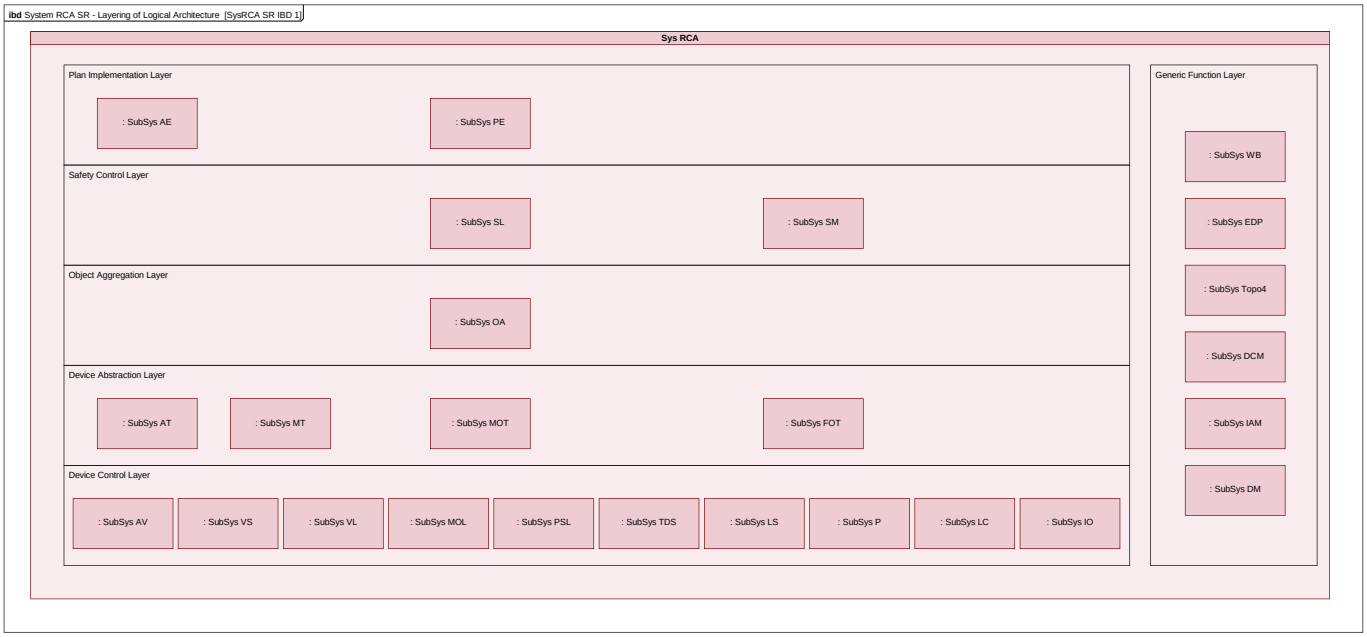


Figure 1 System RCA SR - Layering of Logical Architecture [SysRCA SR IBD 1]

Description: The Reference CCS architecture is divided into architectural Layers. Architectural Layers play an important role in structuring architectures and have successfully been used in computer architecture, communication architecture, etc. In RCA, every Layer has subsystems, and may have special design rules for interfaces (generic for all blocks in the layer) and especially special “abstraction levels”. Example: On the device control layer a function will know about the type of hardware (Point, Level Crossing, Train Detection System) it controls. On the safety control layer “objects” are only known by their abstract hardware independent capabilities (e.g., “trafficability on a node-edge-model”). RCA subsystems are assigned to exactly one layer. System RCA SR - Layering of Logical Architecture [SysRCA SR IBD 1] shows how architectural Layers are applied in the logical architecture of Sys RCA. The Layers are described in the following section.

Plan Execution Layer: Logical components in the plan execution layer execute Operational Plans by generating discrete commands to individual Formations and to abstract objects representing Field Elements in the infrastructure. They use the execution state of the railway to determine the timing of their commands. They report the state of the execution of Operational Plans externally to the Planning System. Logical components in the Plan Execution Layer:

- function independently of the availability of systems generating Operational Plans
- are not concerned with analysis or decision-making
- operate in real-time.

Safety Control Layer: Logical components in the safety control layer ensure a safe future state of the railway by validating that commands lead to a safe state of the railway given the current state of the railway, allowing validated commands to reach the Object Abstraction Layer, and reacting to unsafe states of the railway. Logical components in this layer:

- execute combinations of logical functions on strictly abstract representations of real world elements

- implement rules only through parameter values in abstract objects, not through specialised functions

- operate in real-time

- enable modular safety by decoupling the specific behaviour of individual devices from the abstract logic used on this layer

Object Aggregation Layer: Logical components in the object aggregation layer route and disaggregate abstract object commands to abstract device commands, and aggregate current states from abstract devices into abstract objects. Logical components in this layer:

- operate on strictly abstract representations of real-world elements

- operate in real-time

- implement rules only through parameter values in abstract objects, not through specialised functions

Device Abstraction Layer: Logical components in the device abstraction layer translate between commands and current states of the abstract devices, and those of specific devices. Logical components in this layer:

- in some cases, implement functionality and interfaces defined in the CCS TSI or EULYNX specifications

- operate in real-time

- enable modular safety by decoupling the specific behaviour of individual devices from the abstract logic used on this layer

Device Control Layer: Logical components in the device control layer translate specific device commands into physical output to the controlled device. They also monitor the physical state of the controlled device and report this current device state. Logical components in the Device Control Layer provide maintenance and diagnostics functions for the controlled devices. Logical components in this layer:

- operate in real-time

- are specific to types and versions of device

- in some cases, use (without redefining) functionality and interfaces defined in the CCS TSI or EULYNX specifications

Generic Function Layer: Logical components in the generic function layer provide common capabilities needed by logical components in more than one of the other layers, including interaction with the human users and maintainers of the system, configuration and diagnostic data management, and access to single-source data.

Logical components in the device control layer:

- are not always operational all the time; they are sometimes only used when the system is partially or fully out of operation

- implement, where appropriate, interface protocol stacks defined in the EULYNX specifications

3.2. Authentication/Authorisation Interfaces

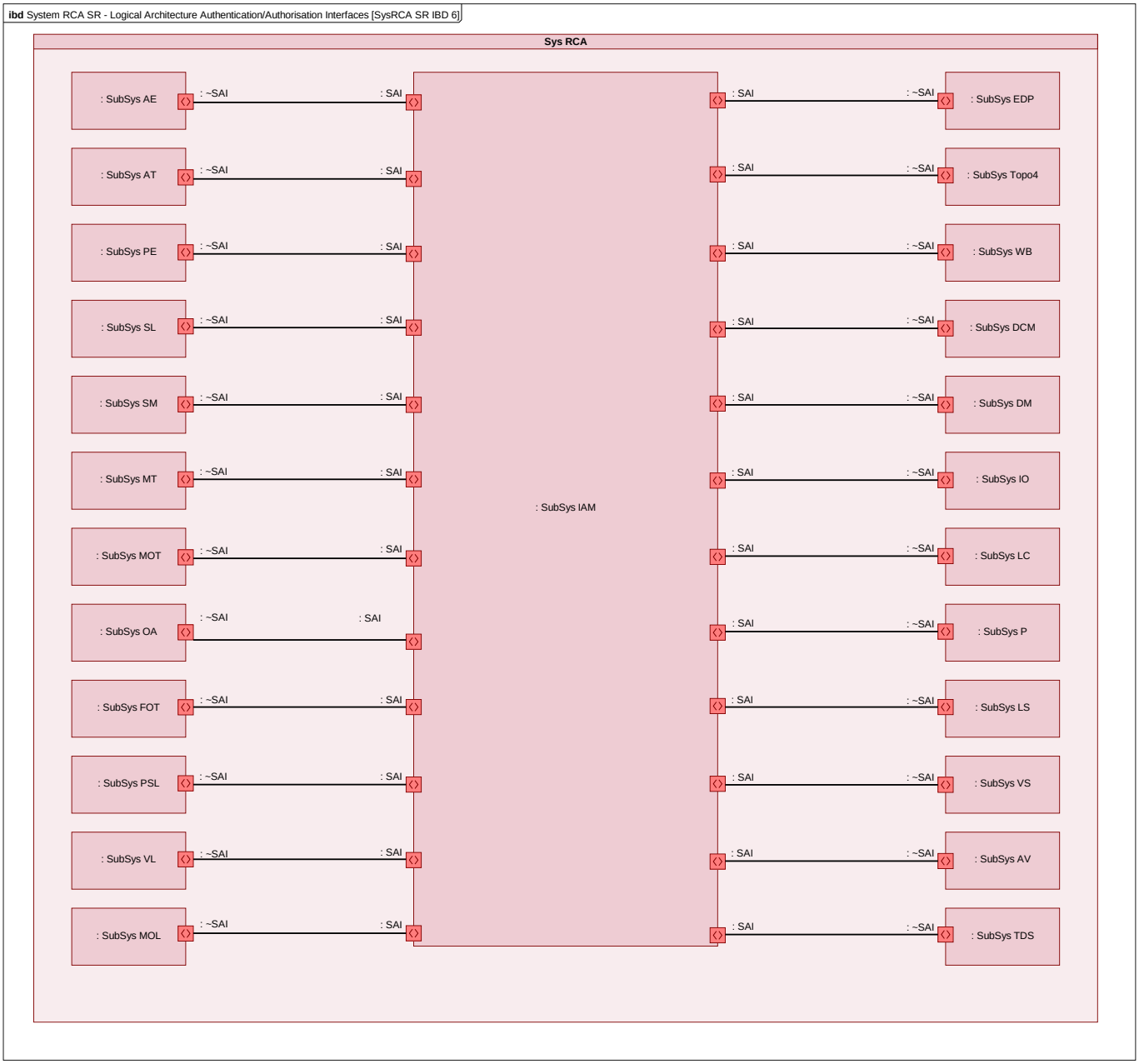


Figure 2 System RCA SR - Logical Architecture Authentication/Authorisation Interfaces [SysRCA SR IBD 6]

Description: System RCA SR - Logical Architecture Authentication/Authorisation Interfaces [SysRCA SR IBD 6] shows the identity and access management interfaces in the logical architecture of Sys RCA.

3.3. Configuration Management Interfaces

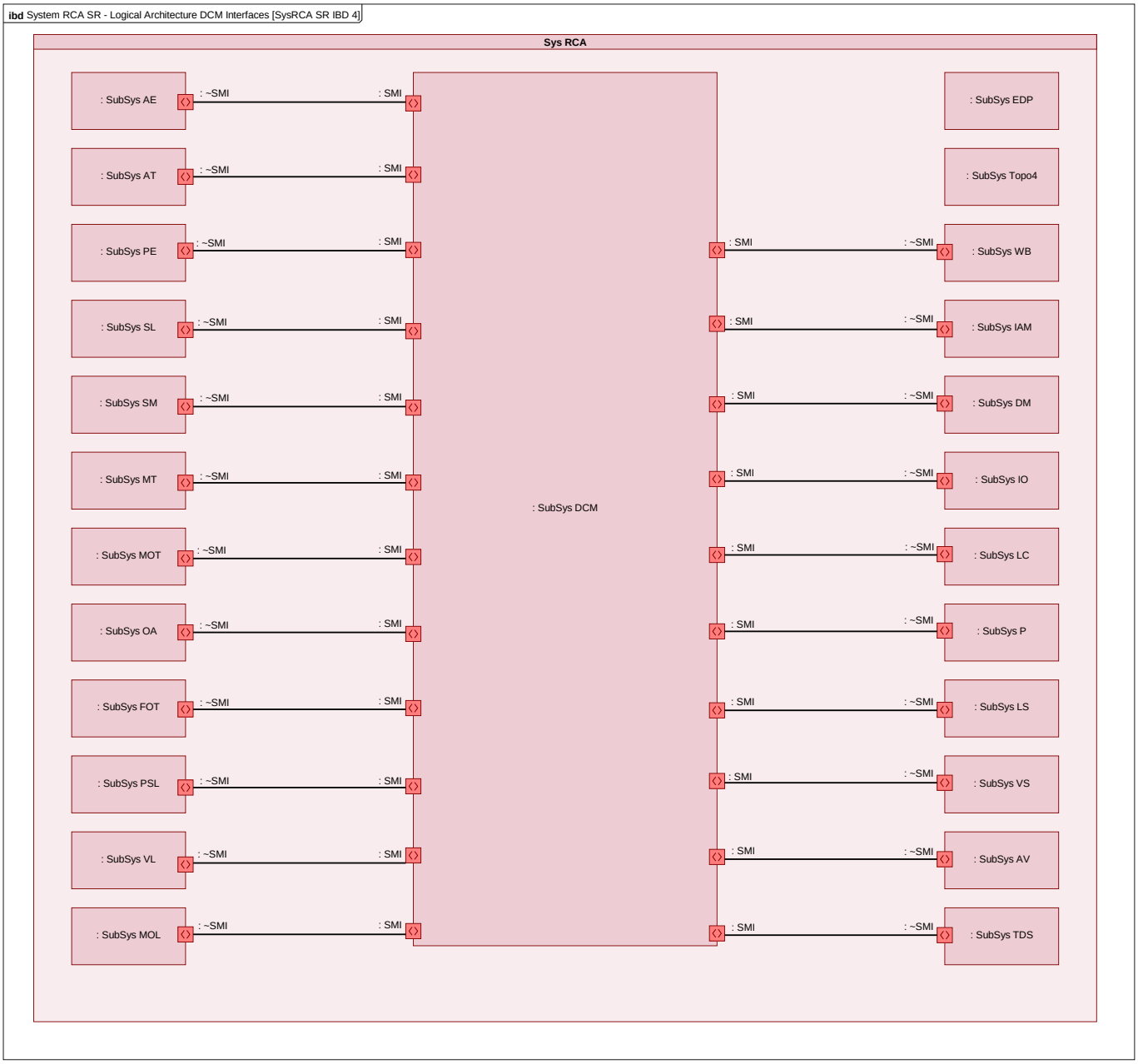


Figure 3 System RCA SR - Logical Architecture DCM Interfaces [SysRCA SR IBD 4]

Description: System RCA SR - Logical Architecture DCM Interfaces [SysRCA SR IBD 4] shows device and configuration management interfaces in the logical architecture of Sys RCA.

3.4. Diagnostic Monitoring Interfaces

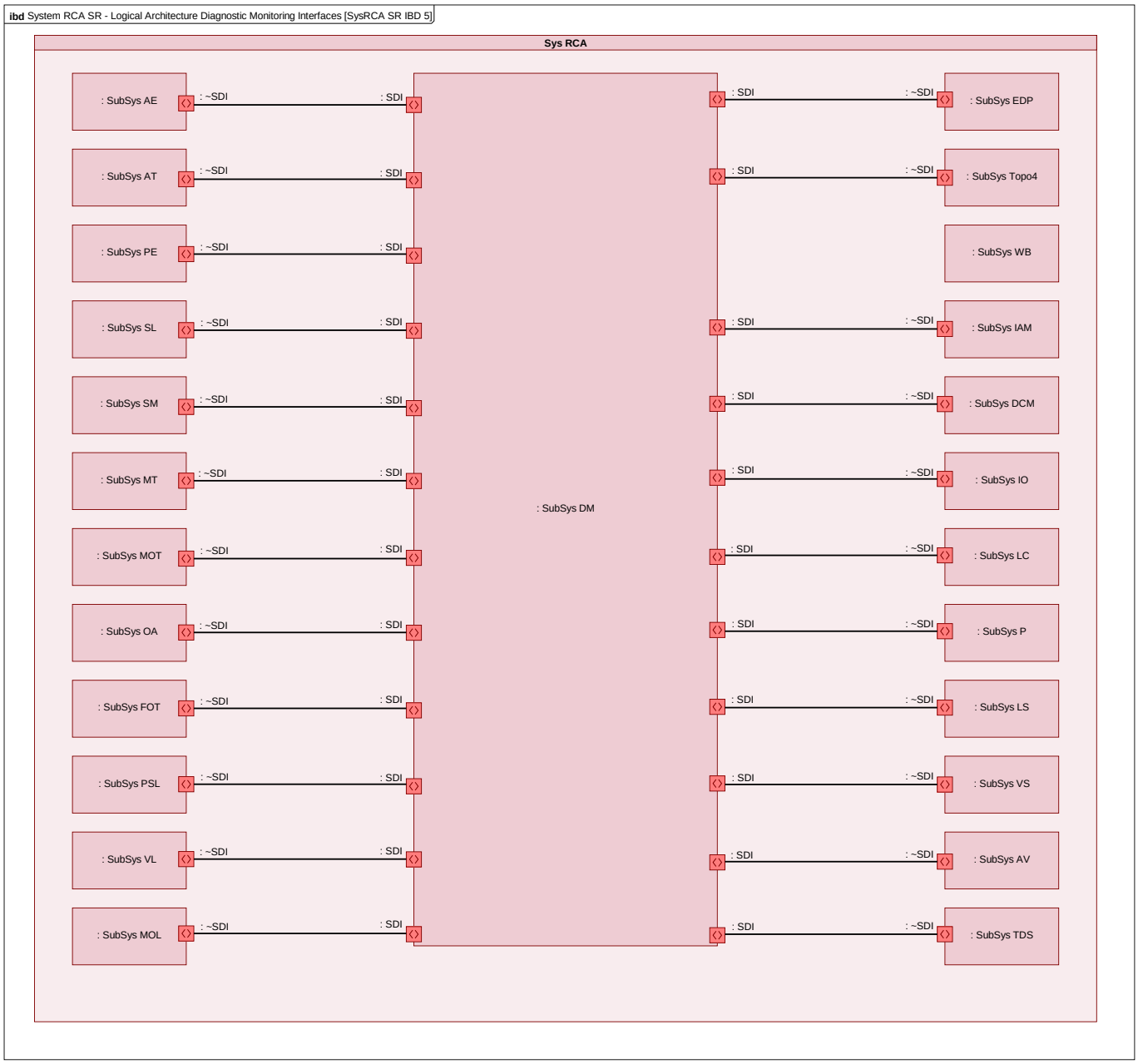


Figure 4 System RCA SR - Logical Architecture Diagnostic Monitoring Interfaces [SysRCA SR IBD 5]

Description: System RCA SR - Logical Architecture Diagnostic Monitoring Interfaces [SysRCA SR IBD 5] shows diagnostic and monitoring interfaces in the logical architecture of Sys RCA.

3.5. Functional Interfaces

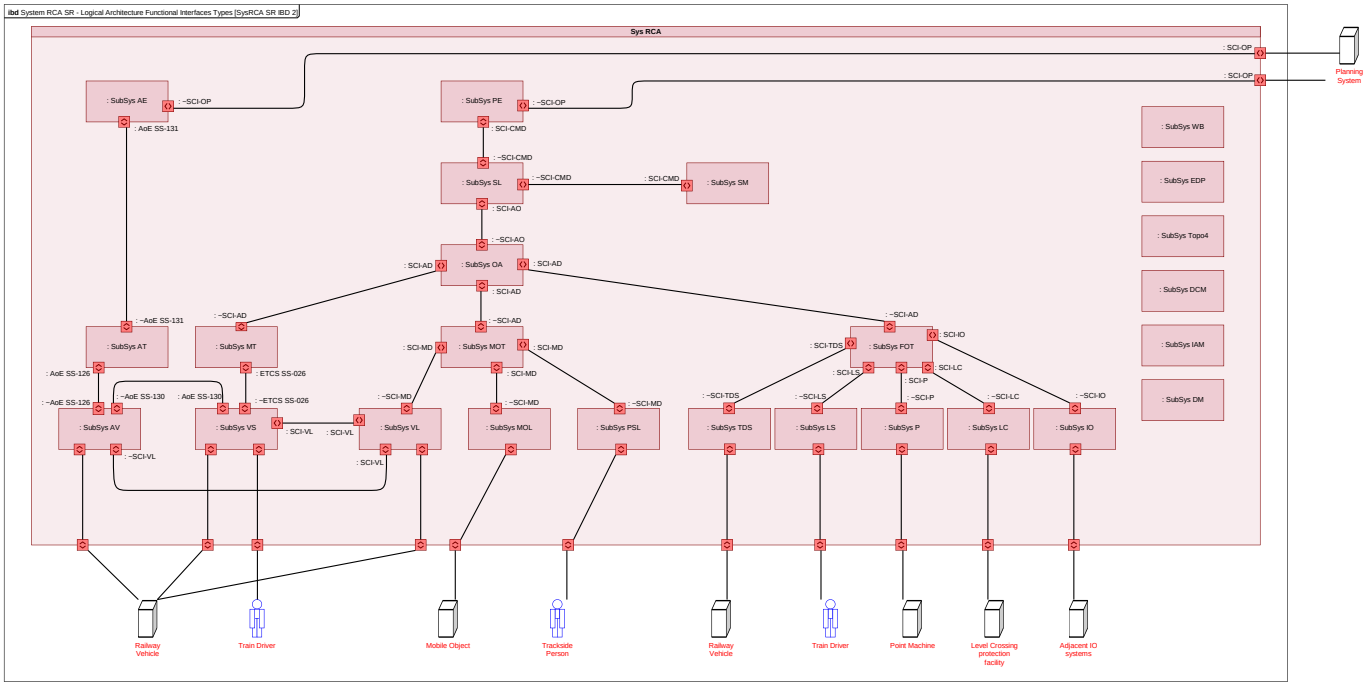


Figure 5 System RCA SR - Logical Architecture Functional Interfaces Types [SysRCA SR IBD 2]

Description: System RCA SR - Logical Architecture Functional Interfaces Types [SysRCA SR IBD 2] shows the different types of functional interfaces in the logical architecture of Sys RCA. Please note: only those actors relevant to the functional interfaces of Sys RCA are depicted on this diagram.

3.6. Workbench Interfaces

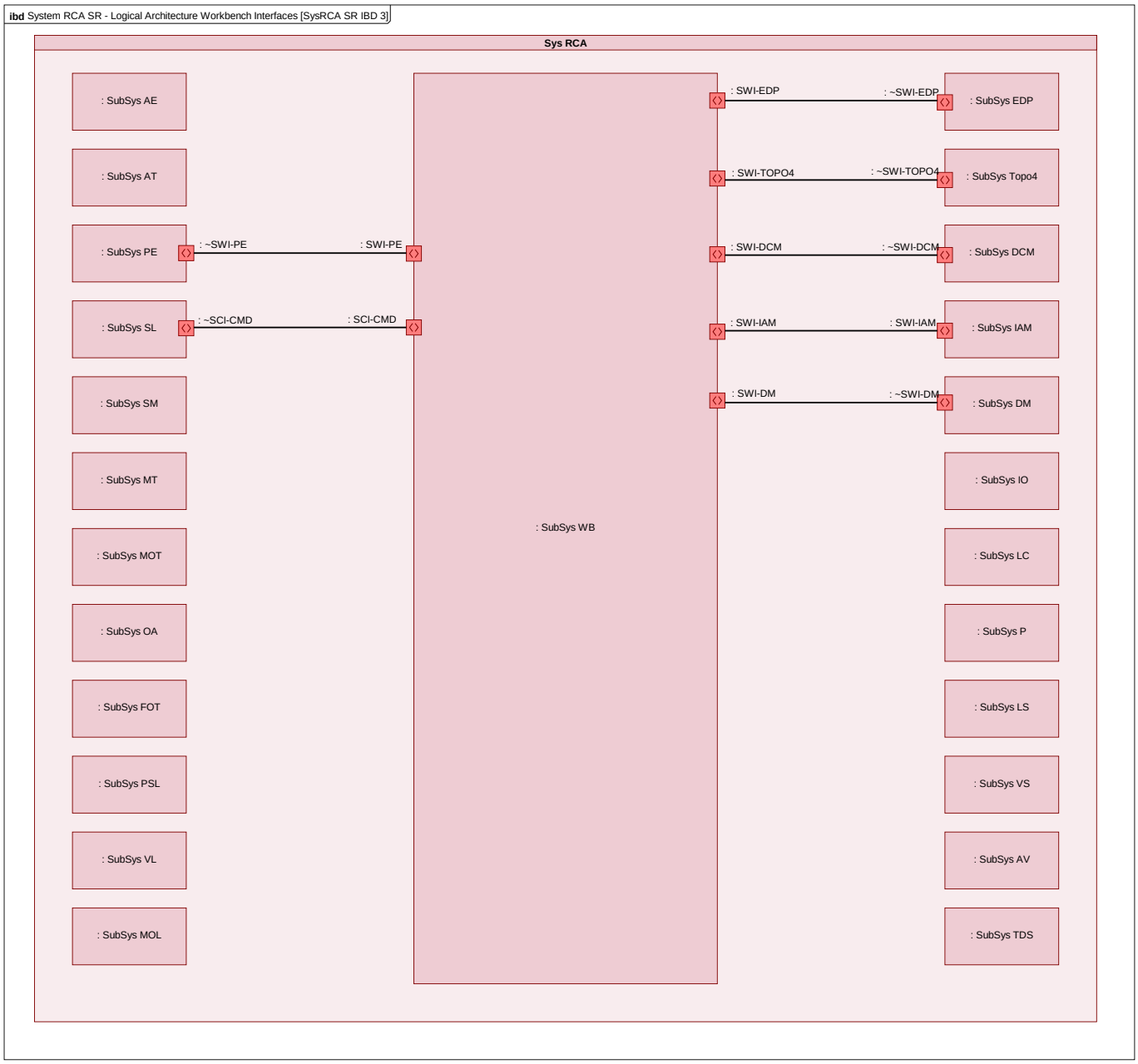


Figure 6 System RCA SR - Logical Architecture Workbench Interfaces [SysRCA SR IBD 3]

Description: System RCA SR - Logical Architecture Workbench Interfaces [SysRCA SR IBD 3] shows the workbench interface in the logical architecture of Sys RCA.

3.7. RCA Subsystems

Description: Sys RCA is composed of several subsystems. This section contains the description of all subsystems of Sys RCA. The subsystems will be specified by dedicated specification documents. Refer to RCA.Doc.6.

3.7.1. SubSys MT

Description: Full name Movement Authority Transactor. The SubSys MT translates commands and state feedback between the device-specific track-train message set (specified in chapter 8.6 of CCS TSI ETCS SUBSET-026) and the abstract objects used on interface SCI-AD. Characteristics:

- The information translated are: Movement Permission to Movement Authority and Train Position Report to LocalisationReportEvent
- Operates in real-time
- For communication between SubSys MT and SubSys VS only radio connection is supported. EUROBALISE are not supported for communication.

3.7.2. SubSys OA

Description: Full name Object Aggregation. SubSys OA routes and disaggregates abstract commands to the appropriate transactor subsystems in the Device Abstraction Layer and aggregates state from subsystems in the Device Abstraction Layer into abstract representations of the state of the railway operation.

Characteristics:

- Operates on strictly abstract representations of real-world elements.
- Operates in real-time.

3.7.3. SubSys SL

Description: Full name: Safety Logic. SubSys SL grants or rejects requests for state changing of either a Field Element or for a planned movement, based on a safety evaluation. The evaluation will be done against safety parameters contained in the abstract objects that represent the state of the railway operation. Where a request is confirmed to be safe, the SubSys SL grants the requested change and issues commands over interface SCI-AO to realise the request. If the request is evaluated as unsafe, the SubSys SL rejects the request and leaves all state unchanged. SubSys SL is responsible for safe movements within a defined Area of Control.

Characteristics:

- Operates on strictly abstract representations of real-world elements
- Operates in real-time

3.7.4. SubSys SM

Description: Full name Safety Manager. SubSys SM monitors the state of the railway operation in the Area of Control, recognises hazardous combinations of states, and triggers safety reactions by issuing commands over interface SCI-CMD.

Characteristics:

- Operates on strictly abstract representations of real-world elements
- Rules for what constitutes a danger pattern are parameterised in the abstract objects
- Operates in real-time

3.7.5. SubSys VS

Description: Full name: Vehicle Supervisor. The SubSys VS implements the supervision part of the ETCS On Board Unit. It enforces the Movement Authority and speed restrictions for a single train. It provides the current train position. The ETCS On Board Unit is specified by several ETCS SUBSETs.

Characteristics:

- Implements the ETCS interface CCS TSI ETCS SUBSET-026 radio message set
- Interacts with other train equipment via the CCS TSI ETCS SUBSET-119
- Operates in real-time
- SubSys VS is a part of the vehicle-borne On Board Unit

3.7.6. SubSys PE

Description: Full name Plan Execution. SubSys PE translates Operational Plans into discrete requests for Movement Permissions and state changes of abstract objects representing Field Elements. SubSys PE coordinates dependencies between concurrently executed Operational Plans and triggers requests based on the current railway operation state. It maintains and provides over its external interface SCI-OP a consolidated, consistent railway operation state to systems outside of Sys RCA.

Characteristics:

- operates on abstract representations of real-world elements
- operates in real-time
- functions independently of business rules (business rules are expressed in the parameter values of Operational Plans and requests)
- functions independently of the availability of Planning System

3.7.7. SubSys AE

Description: Full name: ATO Execution. The SubSys AE translates Operational Plans into Journey Profiles for automatic train operation. SubSys AE supports different GoA. For GoA 2 SubSys AE generates Journey Profiles for automatic train driving. In case of GoA 4 the generated Journey Profile provides additional information for full automatic train operation processes. This will include for example the train door control. SubSys AE also adds necessary supporting information such as topology to the Journey Profile.

Characteristics:

- operates on abstract representations of real-world elements
- operates in real-time
- functions independently of business rules (business rules are expressed in the parameter values of operational plans and requests)

3.7.8. SubSys MOT

Description: Full name: Mobile Object Transactor. SubSys MOT translates between the abstract objects used by the Object Abstraction Layer and the device-specific commands from subsystems on the Device Control Layer and vice versa. It supports location devices with calibration data and provides LocalisationReportEvents. It transfers warnings about planned movements to affected warning devices.

Characteristics:

- Operates in real-time
- Communicates strictly abstract object information to interface SCI-AD

3.7.9. SubSys FOT

Description: Full name: Fixed Object Transactor. SubSys FOT translates between the abstract objects used by the Object Abstraction Layer and the device-specific commands from EULYNX subsystems SubSys P, SubSys LC, SubSys IO, SubSys TDS, SubSys LS on the Device Control Layer and vice versa.

Characteristics:

- Uses EULYNX interfaces toward the Device Control Layer
- Enables modular safety by decoupling the specific behaviour of individual devices from the abstract objects used at the Safety Control Layer
- Operates in real-time

3.7.10. SubSys MOL

Description: Full name: Mobile Object Locator. SubSys MOL provides the position of a trackbound or non-trackbound object on the railway network topology.

Characteristics:

- Operates in real-time
- Operates on one individual object
- Can be implemented using different localisation technologies

3.7.11. SubSys PSL

Description: Full name: Person Supervisor & Locator. SubSys PSL provides warnings and protection from approaching Movable Objects, along with information about their location on the railway network topology received from SubSys MOL, to an individual Trackside Person or a group of Trackside Persons. SubSys PSL can be realised as a tag, a Trackside Person safety system or an app on a mobile device that interacts with the person..

Characteristics:

- Operates in real-time
- Operates on one individual object
- Can be implemented using different localisation technologies

3.7.12. SubSys VL

Description: Full name: Vehicle Locator. SubSys VL uses mobile localisation technology to safely and reliably provide position, length and speed information of the Railway Vehicle. For safe length different options are possible: Either the train integrity or SubSys MOL at the other end of the Trackbound Movable Object will be used. It may emulate a location balise for interfacing ETCS.

Characteristics:

- Operates in real-time
- Can be implemented using different localisation technologies, from today's balise + odometry to additional sensor inputs such as GNSS or inertial measurement units
- SubSys VL is a part of the vehicle-borne On Board Unit

Design Rationale: The rationale for splitting up SubSys VS and SubSys VL functions is done to take in account the different lifecycles.

3.7.13. SubSys AT

Description: Full name ATO Transactor. SubSys AT distributes automatic train operation Journey Profiles, to the On Board Unit of individual Railway Vehicles. It provides status information and execution progress in the form of Status Report Packet (STR) received from the On Board Unit. It handles Journey Profile Request Packet (JPReq) and Segment Profile Request Packet (SPReq). It translates Operational Plans into Journey Profile Packet (JP) and Segment Profile Packet (SP) as specified in CCS TSI ATO over ETCS SUBSET-126.

Characteristics:

- One SubSys AT instance provides functionality to more than one individual Railway Vehicle
- Operates in real-time

3.7.14. SubSys AV

Description: Full name: ATO Vehicle. SubSys AV executes Journey Profile Packet (JP) and Segment Profile Packet (SP) by controlling the physical functions of the Railway Vehicle.

Characteristics:

- Operates on one specific train
- Operates in real-time
- SubSys AV is a part of the vehicle-borne On Board Unit
- Does not have a safety function. Safety supervision will be done by the adjacent SubSys VS

3.7.15. SubSys WB

Description: Full name: Workbench. SubSys WB is a platform for providing process specific user interfaces. User interface can be registered to WB statically and dynamically.

Characteristics:

- SubSys WB isolates the functional logic and user processes
- SubSys WB can handle safe and unsafe user interfaces

3.7.16. SubSys EDP

Description: Full name: Engineering & Data Preparation. SubSys EDP supports commissioning and maintenance processes. It provides topology, engineering and configuration data for all the subsystems of Sys RCA. It highly automates the process of capturing and validating the data.

Characteristics:

- SubSys EDP provides standardised interfaces towards other Sys RCA subsystems

3.7.17. SubSys Topo4

Description: SubSys Topo4 provides a correct, validated topology and topography data for SIL4 systems by combining information from different sources.

Characteristics:

- SubSys Topo4 provides standardised interfaces towards Sys RCA.

3.7.18. SubSys DCM

Description: Full name Device & Configuration Management. SubSys DCM is used to register, setup, and manipulate Devices. This includes distributing and updating the configuration data and the software version to the RCA subsystems.

Characteristics:

- SubSys DCM might be standardised only partially. While it provides standardised interfaces (SMI) towards Sys RCA, its functions will not be fully specified by RCA
- Safety criticality: SubSys DCM is safety critical in so far, that part of the subsystem configuration data is safety critical.

3.7.19. SubSys DM

Description: Full name: Diagnostics & Monitoring. SubSys DM collects monitoring and diagnostics information from systems such as Sys RCA subsystems, Field Element or the Railway Vehicles. The information is on one side used to derive capacity limitation and an estimated duration of the capacity limitation that is used in Planning System to reschedule Operational Plans. On the other side the information is forwarded to a monitoring system of the IM, which triggers the corrective maintenance actions.

Characteristics:

- SubSys DM might be standardised only partially. While it provides standardised interfaces (SDI) towards Sys RCA, its functions will not be fully specified by RCA.

3.7.20. SubSys IAM

Description: Full name: Identity and Access Management. The SubSys IAM authenticates and authorizes users and technical systems and grants or denies access to Sys RCA. Therefore, it will need to store the credentials to authenticate the entities.

Characteristics:

- It supports the implementation of an ISO27001/IEC 62443 compatible architecture.

3.7.21. SubSys TDS

Description: Full name: Train Detection System. The SubSys TDS monitors the vacancy and occupancy status of TVP sections. SubSys TDS receives the status of the TVP sections and may force TVP sections to clear. Refer to EULYNX_Eu.Doc.43.

3.7.22. SubSys LS

Description: Full name: Light Signal. The SubSys LS transmits information to Train driver and Adjacent Signalling System. They are classified into signals at the track (stationary signals) and non-stationary signals. The SubSys LS just refers to stationary signals at the track, which can be set and show the visual signal aspect on the basis of a command or on the basis of a safety-related reaction. Refer to EULYNX Eu.Doc.32.

3.7.23. SubSys P

Description: Full name: Point. The SubSys P is used to control and monitor the Point machines of moveable elements based on a request from the SubSys FOT. Refer to EULYNX_Eu.Doc.36.

3.7.24. SubSys LC

Description: Full name: Level Crossing. The SubSys LC protects the crossing area of rails and vehicles through its Level Crossing protection facility. Refer to EULYNX Eu.Doc.39.

3.7.25. SubSys IO

Description: Full name: Generic IO. SubSys IO is used for integrating signalling systems (identified as adjacent IO systems), controlled and monitored by SubSys FOT. Refer to EULYNX_Eu.Doc.45.

3.8. Interfaces

3.8.1. ETCS SS-026

Description: ETCS SS-026 is the existing ERTMS interface (ETCS trackside-ETCS OBU) with additional functions that are necessary for RCA. Required change requests will be handled using the established CR processes. An example for such a CR would be inclusion of additional

train data from the vehicle “upwards” e.g. the current brake capabilities (for lambda and gamma trains). Refer to CCS TSI ETCS SUBSET-026.

3.8.2. SCI-MD

Description: Full name: Mobile Device Interface. SCI-MD is used to communicate with the different types of mobile Device. The interface provides the position of the Device, requests the Device to output a warning signal and provides additional information to the Device. SCI-MD provides information to the Device, which it needs to localise itself.

Downstream:

- Requests the Device to issue a warning

Upstream:

- Provides the position of the Device

3.8.3. SCI-AO

Description: Full name: Abstract Object Interface. This interface provides commands to control abstract objects and status change messages about of abstract objects. An abstract object represents one or more real-world objects, such as Field Elements and Movable Objects.

Downstream:

- Requests the required allocation state of the elements in a route (e.g. Field Element)
- Grant Movement Permission to the Trackbound Movable Object
- Warn Movable Object (e.g. Trackside Person)

Upstream:

- Provides the current allocation state updates of the elements in a route (e.g. Field Element).
- Provides the position and the extent of Trackbound Movable Object.

3.8.4. SCI-CMD

Description: Full name: Command Interface. SCI-CMD is an interface for controlling the trackside Command Control and Signalling system by discrete commands. It allows the non-safety critical systems to request state changing of either a Field Element or for a planned movement from the SubSys SL. SCI-CMD provides information about the current state of the railway operations.

Downstream:

- Request required Drive Protection Section state of the elements in a route (e.g. Field Element)
- Request Movement Permission for a Trackbound Movable Object
- Request Usage Restriction Area
- Request Warning e.g. for a Train Driver or Trackside Person

Upstream:

- Provides the current allocation state (updates) of the elements (e.g. Field Element)

- Provides the state, position and extent of the Movable Object
- Provides Usage Restriction Area
- Updates about actions taken by SubSys SM

3.8.5. SCI-OP

Description: Full name: Operational Plan Interface. SCI-OP provides Operational Plans from the planning system to the Command Control and Signalling system for the execution. It returns the execution status of the Operational Plans. Operational Plans may be used for the track-precise, timed planning of railway operations, such as train runs, shunting movements, stabling and usage restrictions. SCI-OP supports the update of Operational Plans that are already in execution. The execution status covers planned movements as well as unplanned capacity restrictions (e.g. unavailable track due to a failure).

Downstream:

- Operational Plan

Upstream:

- Execution status

3.8.6. SCI-AD

Description: Full name: Abstract Device Interface. This interface is a single device-oriented interface, which provides access to the transactors. Through this interface a transactor can be controlled and the status monitored.

Downstream:

- Requests the required Drive Protection Section state of the elements (e.g. Field Element)
- Grant Movement Permissions directly to the Trackbound Movable Object or indirectly via a trackside signal.
- Warn a Movable Object (e.g. Trackside Person)

Upstream:

- Provides the current allocation state (updates) of the elements (e.g. Field Element).
- Provides information about the position and extent of a Trackbound Movable Object. The information can already be assigned to a Resolved Trackbound Movable Object or be just location based without an assignment to a Trackbound Movable Object (e.g. Occupancy).

3.8.7. SHI-SL

Description: Full name: SL Handover Interface. The SL handover interface is used to pass a Trackbound Movable Object from one Safety Logic system to the next, adjacent Safety Logic system. Therefore, it must be possible to request a Movement Permission that starts in one Safety Logic system and ends in another instance of a Safety Logic system. The two instances can be from two different IMs or from the same.

NB - Based on an architectural design hypothesis the SHI-SL could be used to interoperate with an existing Interlocking system. This would require an SHI-SL to SCI-ILS adapter. Refer to EULYNX Eu.Doc.41

3.8.8. AoE SS-126

Description: AoE SS-126 interface connects the trackside ATO system to the Railway Vehicle side ATO systems for automatic operation. Refer to CCS TSI ATO over ETCS SUBSET-126.

3.8.9. SCI-VL

Description: Full name: Vehicle Locator Interface. SCI-VL is an interface to safely provide localisation information acquired and computed by Vehicle Locator. SCI-VL is located on the Railway Vehicle and used between subsystems on the Railway Vehicle only.

Upstream:

- Position with confidence intervals
- Speed with confidence intervals
- Acceleration with confidence intervals

3.8.10. AoE SS-130

Description: The AoE SS-130 interface is used between the two Device controllers SubSys AV and SubSys VS to coordinate their parallel Railway Vehicle control. It includes the following information exchange: ATO Status ("AD Mode request", "ATO Engaged"), ETCS Train Data, Dynamic ETCS Data, ETCS supervision information. Refer to: CCS TSI ATO over ETCS SUBSET-130.

3.8.11. SHI-PE

Description: Full name: PE Handover Interface. The SubSys PE handover interface is used between two Plan Execution systems to exchange information about each other's Area of Control and to pass a Movable Object from one Area of Control to the next.

3.8.12. SHI-MOT

Description: Full name: MOT Handover Interface. The SubSys MOT handover interface is used to pass a Movable Object from one Mobile Object Transactor system to the next.

3.8.13. ETCS SS-039

Description: ETCS SS-039 is the ERTMS interface to hand over a Trackbound Movable Object from one Movement Authority Transactor system to the next adjacent Movement Authority Transactor system. Refer to CCS TSI ETCS SUBSET-039.

3.8.14. SHI-IAM

Description: Full name: IAM Federation Interface. Interface which connects different Identity and Access Management systems. It allows safe and secure exchange of authentication and authorisation information.

3.8.15. SCI_R1

Description: Connect an SubSys MT to an ETCS RBC using the ETCS RBC-RBC protocol.

Candidate interface definition: ERTMS SUBSET-039 FIS for the RBC/RBC Handover; ERTMS SUBSET-98/129/26 RBC-RBC Safe Communication Interface

3.8.16. SWI-PE

Description: Full name: PE Workbench. This interface provides input/output functions for user interactions with the Plan Execution system. The Operational Plan, the execution status and all object control requests are part of this interface. This will also be a mobile UI that provides the user interaction for the Personnel at Trackside including but not limited to entering requests (e.g. request a shunting movement) or display current information about next capacity usages.

3.8.17. SWI-TOPO4

Description: Full name: Topo4 Workbench Interface. This interface provides safe input/output functions for user interactions with the SubSys Topo4.

3.8.18. SWI-EDP

Description: Full name: EDP Workbench Interface. This interface provides input/output functions for user interactions with the Engineering & Data Preparation system.

3.8.19. SWI-DCM

Description: Full name: DCM Workbench Interface. This interface provides input/output functions for user interactions with the Device & Configuration Management system.

3.8.20. SWI-IAM

Description: Full name: IAM Workbench Interface. This interface provides safe input/output functions to administrate the identity and access register.

3.8.21. SWI-DM

Description: Full name: DM Workbench Interface. This interface provides input/output functions for user interactions with the Diagnostics & Monitoring system.

3.8.22. SDI

Description: The Diagnostics & Monitoring interface is used between SubSys DM (diagnostics & monitoring) and the monitored Sys RCA subsystems.

Candidate interface definition: EULYNX SDI.

3.8.23. SMI

Description: The Device & Configuration Management interface is used between SubSys DCM and the managed Sys RCA subsystems.

Candidate interface definition: Evolution of EULYNX SMI

3.8.24. SAI

Description: Full name: Authentication/Authorisation Interface. The SAI provides services for authenticating and authorising human user and technical systems.

3.8.25. AoE SS-132

Description: AoE SS-132 is the ATO handover interface used to handover a Railway Vehicle on the trackside from one ATO Transactor to another ATO Transactor. Refer to: CCS TSI ATO over ETCS SUBSET-132.

3.8.26. SHI-SM

Description: Full name: SM Handover Interface. Handover interface between two Safety Manager systems.

3.8.27. SCI-TDS

Description: EULYNX interface, according Interface specification EULYNX SCI-TDS. Refer to EULYNX Eu.Doc.44

3.8.28. SCI-P

Description: EULYNX interface, according interface specification EULYNX SCI-P. Refer to EULYNX Eu.Doc.38

3.8.29. SCI-LC

Description: EULYNX interface, according interface specification EULYNX SCI-LC. Refer to EULYNX Eu.Doc.40

3.8.30. SCI-IO

Description: EULYNX interface, according interface specification EULYNX SCI-IO. Refer to: EULYNX Eu.Doc.46

3.8.31. SCI-LS

Description: EULYNX interface, according interface specification EULYNX SCI-LS. Refer to EULYNX Eu.Doc.33