System Description

Disclaimer

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

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 inthis 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 trademarks 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.

Maintenance

After release, this document immediately enters the maintenance phase. Maintenance includes error corrections and general improvement of the document. Please send your change requests to the following email address: cybersecurity.review@ertms.be

1 Introduction

SUC (System under Consideration): a system of nested systems, each comprising subsystems and components, which together provide the required functionality.

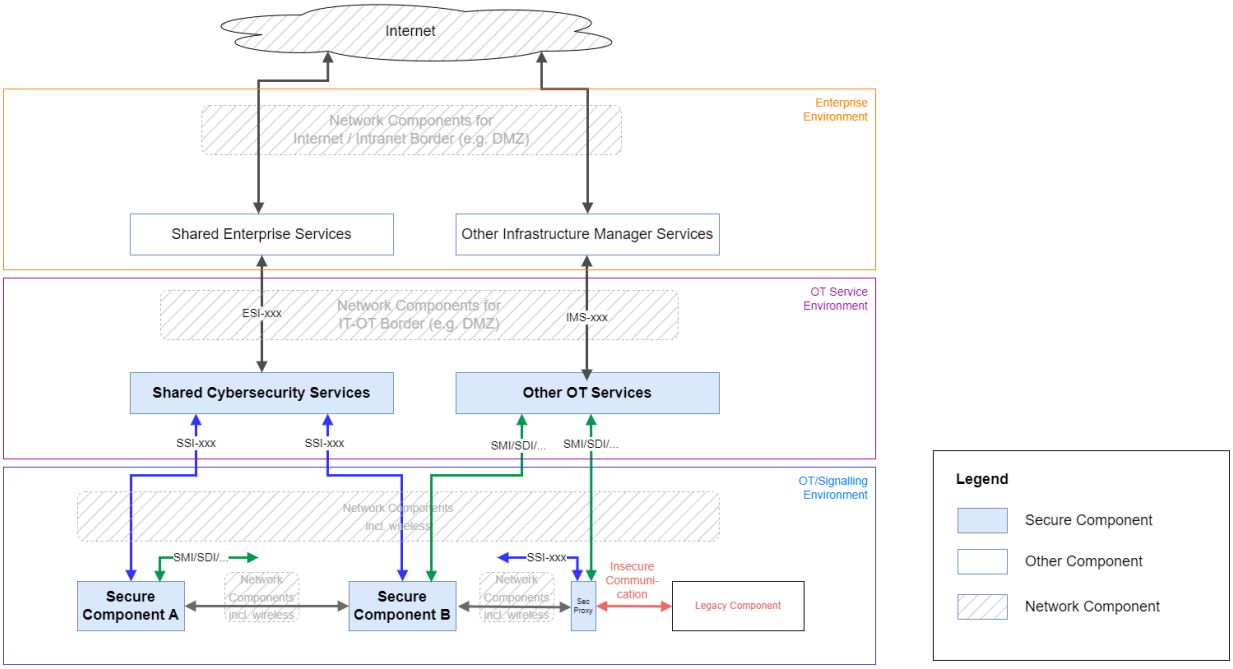
The aim of the SP Cybersecurity specification is to ensure the interoperability of security interfaces across different systems, customer installations and manufacturers.

Implements [IEC PT 63452 ZR-01-01] and the chapter structure following Annex G5.

2 Scope and Boundary

Scope and boundary of the SuC shown in the following figure:

SP-SEC-SysDesc-2-1 - High-level cybersecurity architecture using the key terms of the System Pillar Cybersecurity domain.



In scope of the SuC are:

- the OT/Signalling environment with Secure Components, Network Components, optionally Security Proxies and legacy components
- the OT Service environment with Shared Cybersecurity Services and other OT Services

Out of scope of the SUC are:

- the Enterprise environment with Shared Enterprise Services and other Infrastructure Manager Services
- the Internet and public cloud environments

2.1 Architectural Description

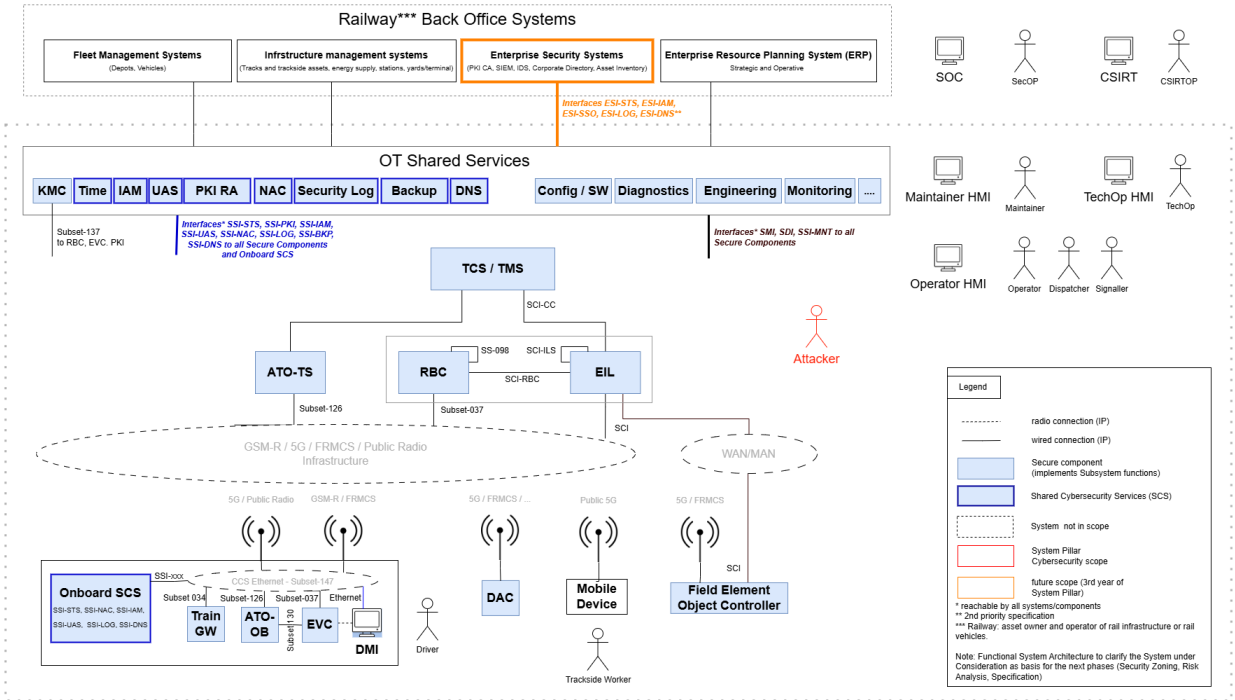
The SuC implements functions to automate train operation.

The different functions of the SuC elements are as follows:

- Secure Components (and legacy components) implement certain automation functions (incl. optionally safety/essential functions)
- Network Components implement network connectivity and optionally filtering functions to allow/disallow communication between Secure Components and communication to SuC external networks and assets.
- Security Proxy is a Network Component to support legacy components to interface with Secure Components
- Shared Cybersecurity Services are centralized security services to providing interfaces to Secure Components
- Other OT Services are centralized services to provide non-security related services to Secure Components

The high-level cybersecurity architecture can be mapped to a detailed architecture, e.g. for a rail automation system:

SP-SEC-SysDesc-2.1-1 - An example of a Cybersecurity Architecture based on definitions in [EULYNX/EU-Rail BL4 R3] and ERA ETCS BL 4.0 for a rail automation system.



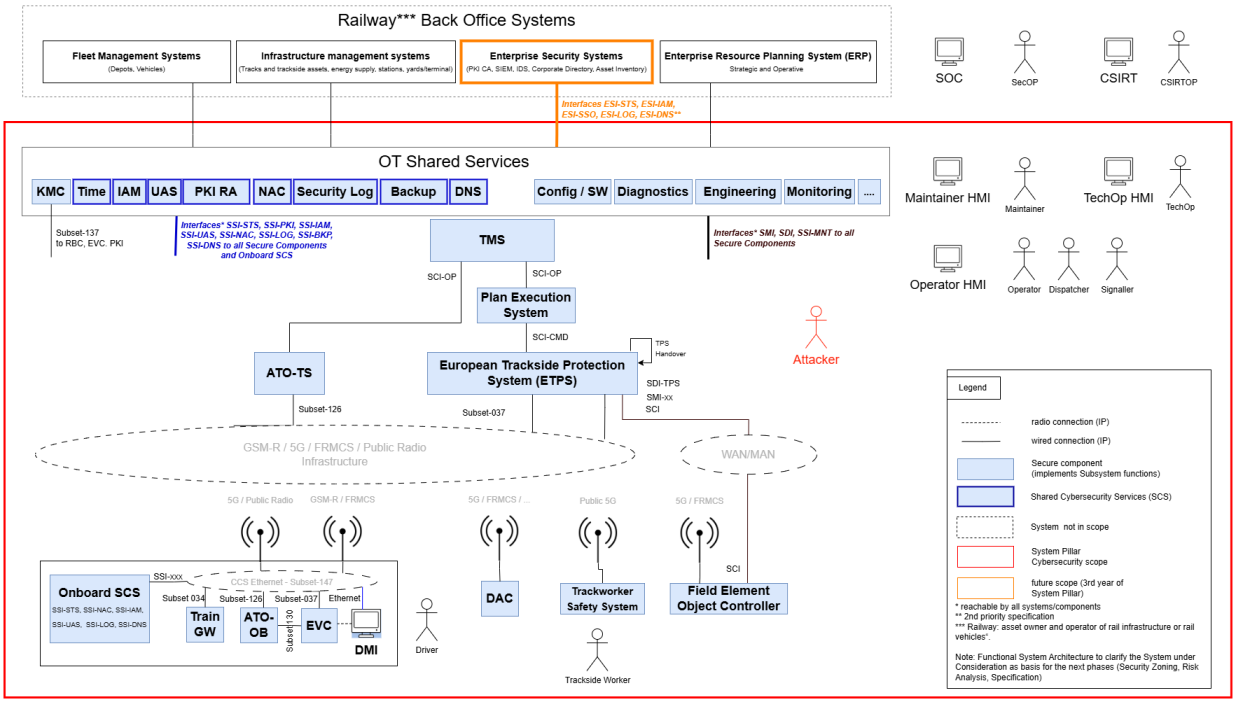
Note: the red rectangular defines the scope of the ERJU System Pillar. The architecture is based on ETCS BL4 and EULYNX BL4 R2 architectures and includes ERJU System Pillar topics as DAC and mobile devices for track-side workers.

In the detailed architecture, the SuC elements are detailed as follows:

- Secure Components are the rail automation assets: TCS/TMS, ATO-TS, RBC, EIL, ATO-OB, EVC, Train-GW, DAC assets, Object Controller, OT Shared Services (Cybersecurity and OT services)
- Network Components are the GSM-R / 5G Modems and routers, the LAN/WAN switches and routers, gateways and firewalls.
- Shared Cybersecurity Services are KMC, TIME, IAM, PKI-RA, NAC, LOG, Backup and DNS.
- Other OT Services are Config/SW Update, Diagnostics, Engineering, Monitoring,...

SP-SEC-SysDesc-2.1-2 - The generic architecture can be also adapted to future version of a rail automation system. The following figures shows newly defined functions from the System Pillar.

SP-SEC-SysDesc-2.1-2.1 - Cybersecurity Architecture for an example rail automation system following the ERJU System Pillar Future Architecture approach based on definitions in [CLS:TS 50701:2023] and [IEC 62443-3-3:2013] .



Note: the red rectangular defines the scope of the ERJU System Pillar. The architecture is based on the solution concept of the Traffic CS System Concept SPT2TRAFFIC-4459.

2.2 Essential Functions

All functions needed to operate the railway system, such as per example traffic control, speed control, traction/brake control,... are considered essential functions.

See following definition:

Essential Function

Function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control (definition from IEC 62443-4-2)

Note: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss

of control and loss of view respectively. In some industries additional functions such as history may be considered essential.
In the context of the ERJU System Pillar all systems in scope provide functionality as defined in "Essential functions".

Note: IEC 63452 definition: All functions needed to operate the railway system, such as per example traffic control, speed control, traction/brake control,...

2.3 Location of installed Components

Location of installed components is relevant for security consideration. The SuC has typically several locations where assets of the SuC are installed: central locations, regional locations, trackside locations and train location.

2.3.1 Central Location

A central location installations are component installations in central buildings and optionally also on a company site.

Typical assets installed in central locations: TCS/TMS systems, as well as the OT Shared Services.

2.3.2 Regional Location

A regional location installation are component installations in regional building (near a station).

Typical assets installed in regional locations are RBC, ATO-TS, EIL systems , although digital communication allows also for central installation. Installations in region locations are typically in a building,

2.3.3 Trackside Location

A trackside location installation are component installations near to the track in cabinets.

Typical assets installed in a trackside location are field element object controllers.

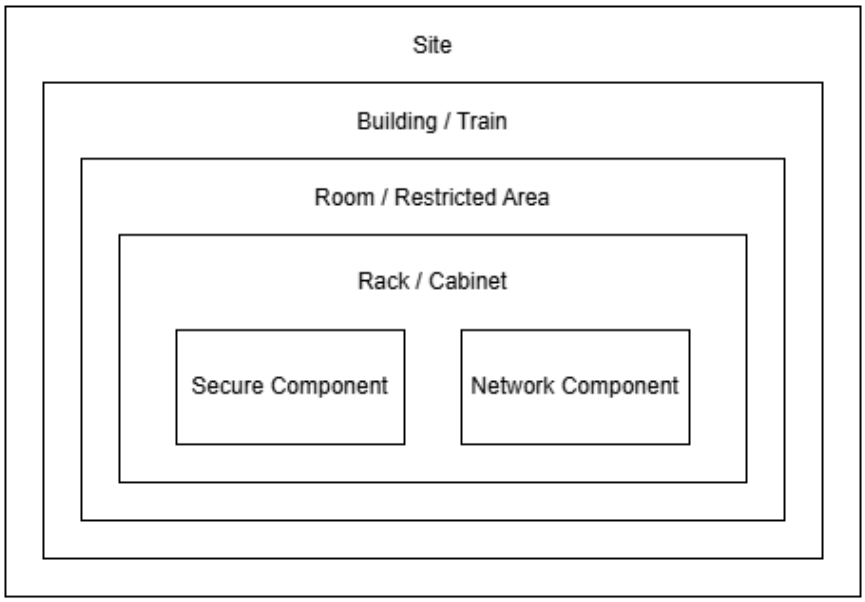
2.3.4 Train Location

A train location installation are component installations on the train.

Typical signalling assets installed on a train: EVC, ATO-OB, DMI, Train-GW, DAC onboard assets.

2.4 Physical Security Perimeter

For the physical security perimeter, the following concept is used:



Physical perimeter concept figure.

Note: Some cabinets are outdoor cabinets in rail automation installation and therefore don't have a surrounding room or building. Trains are usually not protected by a specific site.

2.4.1 - Secure Component Housing

The Secure Component has a physical security perimeter: the housing of the component.

Access to Secure Components is not foreseen during operation or for standard maintenance.

Therefore, following physical protection measures are required by the Secure Component specification:

- a security seal with a unique number which breaks if the housing is opened. This supports the detection of physical intrusion in Secure Components by visual inspection
- electronic tamper detection function which sends a log message when the housing is opened. This supports detection of physical intrusion in Secure Component by online monitoring.

2.4.2 - Installation Rack/Cabinet

A rack or cabinet is an installation place that houses Secure Component and typically also Network Components.

A rack / cabinet has a housing which defines its physical security perimeter.

Access to a rack / cabinet is via the rack / cabinet door.

Following physical security assumptions are made:

- The housing of the rack / cabinet and the access doors / panels withstand intrusion attacks by having attack resistance class of at least RC2 according to EN 1627 (protection against opportunity crimes)

2.4.3 - Installation Room

A room is an installation place that features walls and has for access a door.

For rooms housing critical assets (as Secure Components) it is assumed that:

- the door has access control (either by controlling access to physical keys or by electronic access control). This prevents unauthorized access.
- a forced door alarm in case electronic access control is used.
- the room is supervised using CCTV. This records all activities in the room and can detect internal attackers as well as intruders circumventing the door access control.

2.4.4 - Installation Building/Train

A building is an installation place that has different rooms and has at least on entrance.

A train has installation places in various parts, including restricted and public access areas. Doors and panels protected restricted access areas (e.g. a train driver cabin).

For entrances on building it is assumed:

- the entrance has access control (either by controlling access to physical keys or by electronic access control) or by security personnel. This prevents unauthorized access.
- a forced entrance alarm in case electronic access control is used.
- the entrance is supervised using CCTV. This records all entrances and exits to and from the building and can detect internal attackers as well as intruders circumventing the entrance access control.

For entrances to restricted areas on a train it is assumed:

- the entrance has access control (either by controlling access to physical keys or by electronic access control). This prevents unauthorized access.
- a forced entrance alarm in case electronic access control is used.
- the entrance is supervised using CCTV. This records all entrances and exits to and from the restricted area and can detect internal attackers as well as intruders circumventing the entrance access control.

2.4.5 - Installation Site

An site installation is assumed to be a fenced area that contains one or more buildings. It has one or more entrances.

For the installation site it is assumed:

- The border of the site (e.g. fence) is monitored for breaches, either by electronic means or by security personnel.
- The entrance(s) of the site have access control (either by controlling access to physical keys or by electronic access control) or by security personnel. This prevents unauthorized access.

- A forced entrance alarm in case electronic access control is used.
- The entrance is supervised using CCTV. This records all entrances and exits to and from the restricted area and can detect internal attackers as well as intruders circumventing the entrance access control.

3 Intended Usage

A rail automation system is used to automate train movement and protect trains from safety incidents. It allows for the safe transport of humans and goods via the rail network. To achieve these goals, several functions are required (see next chapter).

4 Descriptions of all Functions

The functions of a (rail) automation system can be divided into the following categories:

1. Essential functions: all functions needed to operate the automation system, such as per example traffic control, speed control, traction/brake control,... (see also definition in Ch 2.2 - Essential functions).
2. Diagnostic functions: all functions needed to diagnose the automation system operation, e.g. diagnostic monitoring, incident monitoring,etc.
3. Maintenance functions: all functions needed to maintain the automation system, e.g. configuration management, trouble shooting, backup and restore. updating, restarting,etc.
4. Engineering functions: all functions needed to commission an automation system: configure, testing, etc.

5 Interfaces / Access Points

The following chapters list the interfaces / access points of the SuC.

5.1 Technical Interfaces

Technical interfaces of the SuC fall in following categories. Functions, protocol and data are described in the referenced detail specifications.

1. Secure Component to Secure Component interfaces: these interfaces are between two Secure Components and are protected using the requirements from the Secure Communication Specification **[SP-SEC-CommSpec]**.
   Impact from initial risk assessment: confidentiality: not relevant, integrity: very high, availability: high

2. Secure Component to Shared Cybersecurity Infrastructure interfaces: these interfaces are listed in the Shared Cybersecurity Services Interface Specification **[SP-SEC-SharedSpec]**
   Impact from initial risk assessment: confidentiality: very high, integrity: very high, availability: middle to very high

3. Secure Component to Maintenance and Diagnostic Services: these interfaces (for the trackside asset scope) are defined in the joint publication from System Pillar and EULYNX Trackside asset specification as SMI and SDI
   Potential impact : confidentiality: very high, integrity: very high, availability: middle to high

4. All other interfaces are considered as other communication interfaces: these interfaces should be secured using the chapter 7 - Securing other communicating interfaces of **[SP-SEC-CommSpec]**
   Potential impact depends on criticality of data in transit

5.2 Human-Machine Interfaces (HMIs)

Human-machine interfaces provide human users with access to technical functionality such as monitor, view, control and change (create, modify, delete). Typical automation systems with HMI are diagnostic system, IAM, MDM, SIEM. TMS, DMI.

These HMIs provides access to functions which control critical aspects of the automation system. Potential impact can be very high (e.g. loss of view, loss of control, loss of essential functions, loss of availability). Therefore, access to these HMIs has to be restricted to authorized users.

Chapter 7.2 of the Secure Component Specification **[SP-SEC-CompSpec]** defines requirements for HMIs.

6 Assets supporting Essential Functions

From the taxonomy used for this SUC, the following asset categories are used, which implement or support the essential functions.

1. Secure Components (automation components): these components implement essential functions. Examples are EVC, RBC, EIL/IXL, object controllers for trackside assets,... These essential functions of these components are protected by applying the requirements from **[SP-SEC-CompSpec],**
2. Shared Cybersecurity Services: these components implement cybersecurity services defined in **[SP-SEC-ServSpec]**. They support the essential functions by supporting and enabling cybersecurity services. These supporting functions are protected by applying the requirements from **[SP-SEC-CompSpec]**.
3. Other OT Services: these component implements other OT services as configuration management, software update, diagnostic monitoring and maintenance services. The support essential functions by ensuring the availability and integrity through maintenance activities. These supporting functions are protected by applying the requirements from **[SP-SEC-CompSpec]**.
4. Network Components: these components implement network functionality as switching, routing and filtering of communication data. They support essential functions by enabling availability. These supporting functions are protected by requirements from Chapter 7.1 from **[SP-SEC-CompSpec]**.
5. Legacy Components: these components do not implement the requirements of [SP-SEC-CompSpec] and may implement essential functions or support essential functions. This poses a higher risk to the otherwise secured automation system. In order to enable legacy components to interact with Secure

Components a translating devices (e.g. Security Proxy) is required. This proxy device is protected by applying the requirements from **[SP-SEC-CompSpec]** on the communication side to the Secure Components. A dedicated risk assessment (initial and detailed) is required to identify the risks introduced by legacy components.

7 Operating Environment

This chapter describes the operating environment and operating scenarios.

7.1 Physical Environment

The physical environment contains the detailed maps, plans, existing wiring schematics and connector configurations, site security plans for the different installation locations of chapter 2.3 of this document.

7.2 Logical Environment

The logical environment is depicted in chapter 2.1 of this document. It can be further detailed and accompanied with a network architecture diagram.

7.3 Constraints

Rail automation systems can have a large geography footprint: they are a country-wide or city-wide infrastructure.

Such a large area is hard to monitor and it is hard to prevent access to infrastructure assets.

The assumptions of installation locations is described in chapter 2.3 of this document.

7.4 Adjacent System Function

Adjacent system functions are neighbouring systems such as other rail automation systems from other geography or administrative area. A dedicated risk assessment (initial and detailed) is required to identify the risks introduced by adjacent systems which may not implement the requirements from **[SP-SEC-CompSpec]**.

7.5 Organisational Interfaces

Several stakeholders have interfaces to the (rail) automation systems. Operators and maintenance personnel, engineers, configuration managers, service personnel.

As such personnel has access to various parts of the rail automation system. certain requirements apply to the organisations and their personnel. Refer to **[SP-SEC-PrgmSpec]** for secure operational process requirements.