EU-RAIL SYSTEM PILLAR

Detailed Risk Assessment

Version: 1.1

Detailed Risk Assessment

Document data

Created by	System Pillar Cybersecurity Domain
Classification	Public
Status	Released
Version	1.1
Date	23-MAR-2026

Copyright

Document History

Version	Date	Description	Status
1.1	23-MAR-2026	Error correction and additional guidance for version 1.0	released
1.0	20-FEB-2025	Initial public release	released

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 Table of Contents

2 Preamble

2.1 Scope, Purpose and Intended Audience

SP-SEC-DRA-2.1-1 - The scope of the detailed risk assesement is based on the generic security architecture. This architecture can be mapped to detailed architectures used in projects. **[**SPPRAMSS-16535 **]**

SP-SEC-DRA-2.1-2 - The detailed risk assessment is part of the reference system applied in the context [CEN-CENELEC TS 50701:2023] and [IEC 63452], together with the SP Cybersecurity Specification main documents and supporting documents. **[**SPPRAMSS-16532 **]**

SP-SEC-DRA-2.1-3 - The intended audience are cybersecurity experts in the rail domain. **[**SPPRAMSS-16533 **]**

SP-SEC-DRA-2.1-4 - This risk assessment will be updated in the next release. **[**SPPRAMSS-16531 **]**

2.2 Document Usage

SP-SEC-DRA-2.2-1 - This detailed risk assessment result can be used when implementing the generic security architecture. **[**SPPRAMSS-16534 **]**

2.3 References

[SP-SEC-SysDesc]
Europe's Rail System Pillar Cybersecurity Domain - System Description v1.1

[ERORAT Guideline]
The main objective of this document is the creation and presentation of Security Risk Assessment for System
Design process. This process is a harmonized and consolidated approach. This guideline was created in collaboration with EULYNX, EUG, RCA and OCORA.

[SP-SEC-ThreatCat]
Europe's Rail System Pillar Cybersecurity Domain - Threat Catalog, v1.1

[SP-SEC-InitRiskAna]
Europe's Rail System Pillar Cybersecurity Domain - Intial Risk Analysis, v1.1

[SP-SEC-DetRiskMatrix]
Europe's Rail System Pillar Cybersecurity Domain - Matrix of the Detailed Risk Assessment v1.1

[IEC 62443-4-1:2018]
Secure product development lifecycle requirements

[CEN-CENELEC TS 50701:2023]
Railway applications - Cybersecurity

[Cyber Resilience Act (CRA)]
Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)

[IEC PT 63452]
Railway applications - Cybersecurity - January 2025 draft

[SP-SEC-DetRiskMatrix]
Europe's Rail System Pillar Cybersecurity Domain - Matrix of the Detailed Risk Assessment v1.1

[SP-SEC-CompSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Component Specification, v1.1

[SP-SEC-CommSpec]
Europe's Rail System Pillar Cybersecurity Domain - Secure Commmunication Specification, v1.1

[SP-SEC-ServSpec]
Europe's Rail System Pillar Cybersecurity Domain - Shared Cybersecurity Services Interface Specification, v1.1

[SP-SEC-PrgmReq]
Europe's Rail System Pillar Cybersecurity Domain - Secure Program Requirements, v1.1

2.4 Terms and Definitions

SP-SEC-DRA-2.4-1 - Terms and definitions are defined in [IEC 63452] **[**SPPRAMSS-16527 **]**

3 Introduction

SP-SEC-DRA-3-1 - The detailed risk assessment for the scope defined in [SP-SEC-SysDesc] was conducted by security experts from SP Cybersecurity domain with particpants from industry and rail operators in January 2026. **[**SPPRAMSS-16529 **]**

SP-SEC-DRA-3-2 - This detailed risk assessement is intended to be reused for a wide range of rail automation projects, since the generic approach can be mapped to detailed scope description without adding additional risk. **[**SPPRAMSS-16526 **]**

4 Operating Environmental Assumptions

SP-SEC-DRA-4-1 - The operating envrionmental assumptions are described in[Ch 7 SP-SEC-SysDescr] **[**SPPRAMSS-16528 **]**

5 Risk Acceptance Criteria

SP-SEC-DRA-5-1 - The acceptable risk level is MEDIUM (scale LOW, MEDIUM, HIGH, VERY HIGH). See [ERORAT Guideline] **[**SPPRAMSS-16530 **]**

6 Threat Environment Evaluation

SP-SEC-DRA-6-1 - The threat envrionment is documented in the Threat Catalog [SP-SEC-ThreatCat]. **[**SPPRAMSS-16525 **]**

7 Zone and Conduits

SP-SEC-DRA-7-1 - The figure below shows the zone and conduits of the generic architecture used in this detailed risk assessment. **[**SPPRAMSS-16536 **]**

SP-SEC-DRA-7-2 - Generic Security Zoning

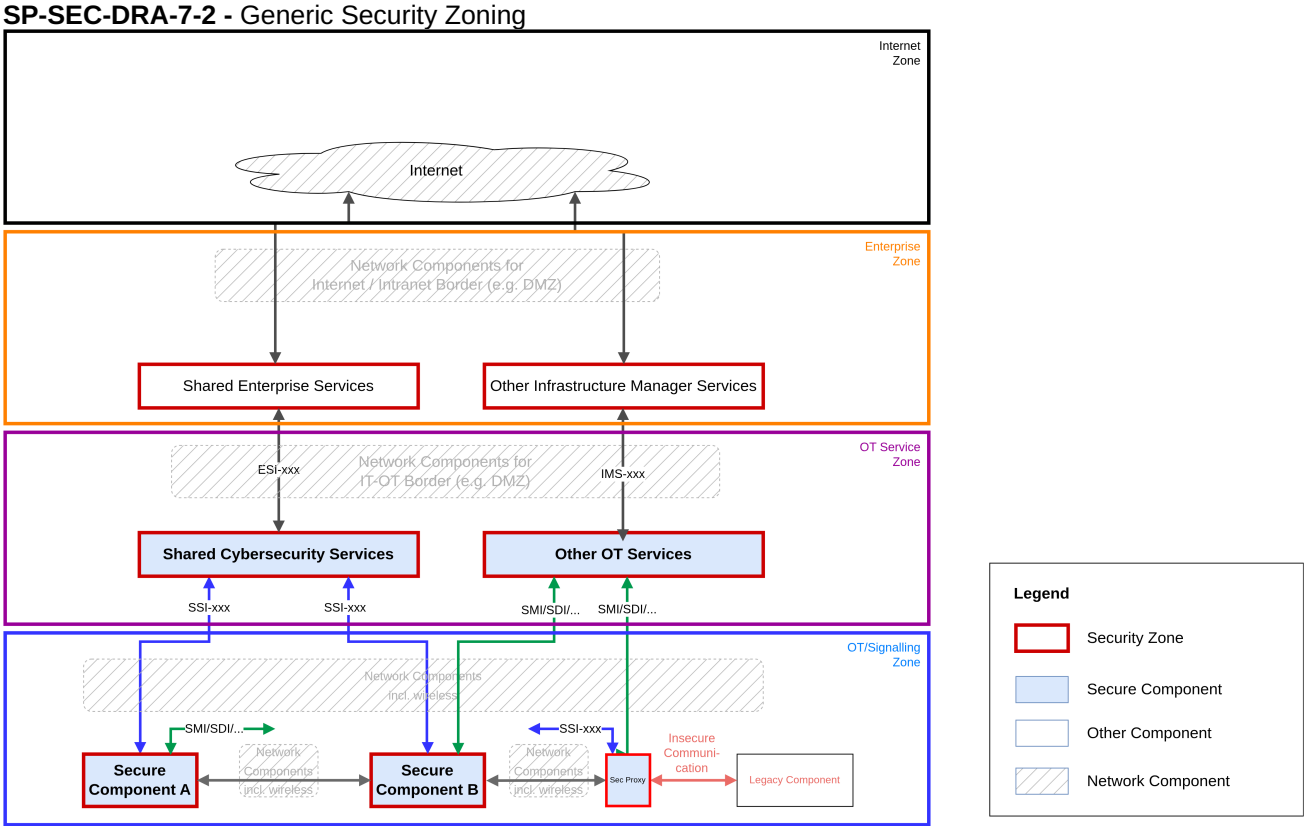

Figure 1 Generic Security Zoning

[SPPRAMSS-10392 **]**

SP-SEC-DRA-7-3 - This detailed risk assessement covers the OT/Signalling Zone with Secure Components and Security Proxy, and the OT Service Zone with Shared Cybersecurity Services and Other OT Services. **[**SPPRAMSS-16552 **]**

SP-SEC-DRA-7-4 - Conduits are the interfaces between the depicted zones. **[**SPPRAMSS-16550 **]**

SP-SEC-DRA-7-5 - The risk assessed is the same for all zones and related conduits. **[**SPPRAMSS-16551 **]**

8 Initial Risks Assessment Result

SP-SEC-DRA-8-1 - The result of the initial risk assessment was VERY HIGH, see [SP-SEC-InitRiskAna]. **[**SPPRAMSS-16548 **]**

SP-SEC-DRA-8-2 - The acceptable and tolerable risk is MEDIUM. **[**SPPRAMSS-16549 **]**

SP-SEC-DRA-8-3 - Additional measures are necessary. The detailed risk assessment resulted in these additional measures. **[**SPPRAMSS-16546 **]**

9 Detailed Risk Evaluation Results

SP-SEC-DRA-9-1 - This detailed risk assessment used the methodology described in [ERORAT Guideline]. **[**SPPRAMSS-16547 **]**

SP-SEC-DRA-9-2 - The result of the detailed risk assessment is that the cybersecurity risk from the threat catalog is reduced to the risk level MEDIUM when applying the countermeasures of chapter 13. **[**SPPRAMSS-16544 **]**

SP-SEC-DRA-9-3 - The result of the detailed risk assessment is documented in [SP-SEC-DetRiskMatrix]. **[**SPPRAMSS-16545 **]**

10 Assumptions

SP-SEC-DRA-10-1 - All assumptions are described in the [SP-SEC-SysDesc]. **[**SPPRAMSS-16541 **]**

11 List of Vulnerabilities

SP-SEC-DRA-11-1 - [EU CRA] mandates to supply only devices without exploitable vulnerabilities. **[**SPPRAMSS-16542 **]**

SP-SEC-DRA-11-2 - Further discovered vulnerabilities are handled by vulnerability management process defined in [IEC 62443-4-1] and Chapter 13.3 of [SP-Sec-PrgmReq]. **[**SPPRAMSS-16543 **]**

12 Unmitigated Risks

SP-SEC-DRA-12-1 - All risks in the threat catalog have been mititgated. **[**SPPRAMSS-16537 **]**

13 List of Countermeasures

SP-SEC-DRA-13-1 - The security countermeasures are documented in the following documents:

- [SP-SEC-CompSpec]
- [SP-SEC-CommSpec]
- [SP-SEC-ServSpec]
- [SP-Sec-PrgmReq]

[SPPRAMSS-16538 **]**

14 Residual Risk

SP-SEC-DRA-14-1 - Residual risks are listed in Chapter 8 of [SP-SEC-CompSpec]. **[**SPPRAMSS-16539 **]**

SP-SEC-DRA-14-2 - All residual risks can be accepted (for risk MEDIUM and LOW) or are mitigated. **[**SPPRAMSS-16540 **]**