EU-RAIL SYSTEM PILLAR

# Initial Risk Assessment

**Version: 1.1**

# Initial Risk Assessment

## Document data

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

## Copyright

© Europe's Rail Joint Undertaking, 2026

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 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.

## 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

1 Table of Contents . . . . . 4
2 SuC Description . . . . . 4
3 Threat Catalogue . . . . . 4
4 Risk Impact Assessment Method . . . . . 4
5 Initial Risk Assessment . . . . . 10

# 2 SuC Description

The definition of the system under consideration (SuC) can be taken from the system description ( System Description )

# 3 Threat Catalogue

The following threat catalogue is used in this version of the specifications: [SP-SEC-ThreatCat]

A future version of this specification can include an updated threat catalogue harmonizing various existing threat catalogues (BSI, ANSSI, MITRE,...).

# 4 Risk Impact Assessment Method

The initial risk assessment is based on the impact assessment method. That method evaluates the worst case impact if an attack is successful. The impact is assessed based on different criteria. These criteria are:

- Confidentiality
- Integrity
- Availability
- Non Repudiation
- Authenticity

Each assessment criteria is evaluated based on different categories of impact. Based on the impact, the level (low - very high) is defined. In the evaluation always the maximum value of the evaluated categories is chosen.

The definitions are listed in the following table.

| Category / Protection class | Financial Impact | Privacy violations | Violation of laws, regulations and rules | Disruption of business activity | Loss of reputation | Health damage |
|---|---|---|---|---|---|---|
| Definition | Loss of revenue, damages, additional personnel costs or investments, material damage, etc. | Handling personal data of customers, employees and suppliers on the basis of the applicable data protection laws and the guidelines applicable thereto.<br>It is strongly recommended to coordinate the assessment with the relevant data protection organisation. | For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc. | Delayed implementation, late delivery, additional expenditure, inadequate service, etc. | Negative reporting, loss of confidence among customers and business partners, etc. | Injuries, fatalaties of humans |
| Low | No or only minor financial damage. Financial thresholds are defined by the CISO or the CEO. | An impairment of the right of self-determination with regard to information has no effect on the right of personality of the person concerned. e.g. generally accessible data, address data within the scope of an employment contract or | The risk occurrence comprises a single issue with politicall y/legally relevant sub-aspects.<br>Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR right to | Increased constraints on operations with acceptable impact on capabilities/ processes.<br>Note: The following aspect may be relevant in the assessment:<br>- End customer service | Country-wide and supra-regional (neighboring countries) critical reporting of sub-areas/individuals of the company.<br>Note: The following aspects may be relevant when assessing reputation: Employee | Individuals may suffer minor injuries if the system fails.. |

| Category / Protection class | Financial Impact | Privacy violations | Violation of laws, regulations and rules | Disruption of business activity | Loss of reputation | Health damage |
|---|---|---|---|---|---|---|
| Definition | Loss of revenue, damages, additional personnel costs or investments, material damage, etc. | Handling personal data of customers, employees and suppliers on the basis of the applicable data protection laws and the guidelines applicable thereto.<br>It is strongly recommended to coordinate the assessment with the relevant data protection organisation. | For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc. | Delayed implementation, late delivery, additional expenditure, inadequate service, etc. | Negative reporting, loss of confidence among customers and business partners, etc. | Injuries, fatalaties of humans |
| | | other contractual relationship, personnel number. | personal self-determination and integrity. | provision - public supply | reputation, employer reputation, strategic target achievement at risk, loss of customers or market share / political trust. | |
| Middle | Tolerable financial damage. The financial thresholds | An impairment of the right to informational self-determination has a minor impact | The occurrence of risk comprises a single issue that leads to | Increased constraints on operations with acceptable | Country-wide and supra-regional (neighboring countries) critical | If the system fails, individuals may suffer |

| Category / Protection class | Financial Impact | Privacy violations | Violation of laws, regulations and rules | Disruption of business activity | Loss of reputation | Health damage |
|---|---|---|---|---|---|---|
| Definition | Loss of revenue, damages, additional personnel costs or investments, material damage, etc. | Handling personal data of customers, employees and suppliers on the basis of the applicable data protection laws and the guidelines applicable thereto.<br>It is strongly recommended to coordinate the assessment with the relevant data protection organisation. | For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc. | Delayed implementation, late delivery, additional expenditure, inadequate service, etc. | Negative reporting, loss of confidence among customers and business partners, etc. | Injuries, fatalaties of humans |
| | are defined by the CISO or the CEO. | on the personal rights of the data subject.<br>e.g. generally accessible data, address data within the scope of an employment contract or other contractual relationship, personnel number. | a contractual, legal or political audit with probable consequences (e.g., penalties).<br>Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR right to | impact on capabilities/ processes.<br>Note: The following aspect may be relevant in the assessment:<br>- End customer service provision<br>- public supply | reporting of sub-areas/individuals of the company.<br>Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic target achievement at risk, | serious injuries. As a rule, inpatient hospitalization is required. |

| Category / Protection class | Financial Impact | Privacy violations | Violation of laws, regulations and rules | Disruption of business activity | Loss of reputation | Health damage |
|---|---|---|---|---|---|---|
| Definition | Loss of revenue, damages, additional personnel costs or investments, material damage, etc. | Handling personal data of customers, employees and suppliers on the basis of the applicable data protection laws and the guidelines applicable thereto.<br>It is strongly recommended to coordinate the assessment with the relevant data protection organisation. | For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc. | Delayed implementation, late delivery, additional expenditure, inadequate service, etc. | Negative reporting, loss of confidence among customers and business partners, etc. | Injuries, fatalaties of humans |
| | | | personal self-determination and integrity. | | loss of customers or market share / political trust. | |
| High | High financial damage. Financial thresholds are defined by the CISO or the CEO. | An impairment of the right to informational self-determination has a significant impact on the personal rights of the person concerned or is a criminal offense. | The occurrence of risk comprises a situation/series of situations that have contractual, legal or political consequence | Extensive constraints in operative operations with high impact on capabilities/ processes or critical facilities.<br>Note: The following | National/international critical reporting. The reputation of the operator is at risk, market shares and new business are at risk. | If the system fails, many people can suffer serious injuries. As a rule, inpatient hospitalization is |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | e.g. customer or employee profiles, qualification or scoring data, wage or salary data, bank data, health data, political and religious convictions, video surveillance and recording, telecommunication service data at the provider. | s for parts of the management.<br>Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR right to personal self-determination and integrity. | aspect may be relevant in the assessment:<br>- End-user service delivery<br>- public supply | Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic goal achievement at risk, customer or market share loss / political trust. | required. Individuals may also be killed by the failure of the system. |
| Very High | Existence-threatening damage. The financial threshold values are defined by the CISO or the CEO. | There is a high need for protection and, moreover, the processing of personal data is an existential business purpose of the company.<br>An impairment of the right to informational self-determination can threaten the existence of the company. For example, personal data that is subject to professional secrecy or bank or credit card accounts at the call | The occurrence of risk comprises a series of circumstances that lead to critical contractual, legal and political consequences for the entire management.<br>Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR right to personal self-determinatio | Large-scale cessation of operations. Capabilities/ processes have been interrupted or are operating below the legal thresholds for critical facilities.<br>Note: The following aspect may be relevant in the assessment:<br>- End customer service provision<br>- Public supply | International negative reporting, image of the company damaged for the long term with all stakeholders.<br>Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic goal achievement at risk, loss of customers or market share / | Fatalities and/or multiple severe injuries |

| Category / Protection class | Financial Impact | Privacy violations | Violation of laws, regulations and rules | Disruption of business activity | Loss of reputation | Health damage |
|---|---|---|---|---|---|---|
| Definition | Loss of revenue, damages, additional personnel costs or investments, material damage, etc. | Handling personal data of customers, employees and suppliers on the basis of the applicable data protection laws and the guidelines applicable thereto.<br>It is strongly recommended to coordinate the assessment with the relevant data protection organisation. | For example: Group guidelines, company agreements, service regulations, legal ordinances, customs regulations, etc. | Delayed implementation, late delivery, additional expenditure, inadequate service, etc. | Negative reporting, loss of confidence among customers and business partners, etc. | Injuries, fatalaties of humans |
| | | centre. | n and integrity. | | political trust. | |

## 5 Initial Risk Assessment

The following initial risk assessment is documented based on the definitions in chapter 2 and 4.

| Requ/ System Name | Secure Component | SCS-STS | SCS-PKI | SCS-UAS | SCS-LOG | SCS-BKP | SCS-IAM | SCS-NAC | SCS-DNS |
|---|---|---|---|---|---|---|---|---|---|
| System ID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Function | Safety related function in CCS according to SuC description | Provide Time for synchronised time | Certificate Management | Single sign on, authentification | collecting and evaluating logs | back up of software and configs, centrally | Identity and access management | Network authentication | Domain name system |
| relevant for safety | yes | yes | no | no | no | no | no | no | no |
| Confidentiality | not relevant | not relevant | very high | very high | very high | not relevant | high | low | low |
| Integrity | very high | high | very high | very high | very high | very high | very high | very high | very high |

| Requ/SystemName | Secure Component | SCS-STS | SCS-PKI | SCS-UAS | SCS-LOG | SCS-BKP | SCS-IAM | SCS-NAC | SCS-DNS |
|---|---|---|---|---|---|---|---|---|---|
| Availability | high | middle | middle | high | high | very high | very high | very high | very high |
| Non-Rep | middle | middle | middle | middle | middle | middle | very high | high | high |
| Authenticity | very high | middle | nr | high | high | high | very high | very high | very high |

| Requ/ System Name | Secure Component | SCS-STS | SCS-PKI | SCS-UAS | SCS-LOG | SCS-BKP | SCS-IAM | SCS-NAC | SCS-DNS |
|---|---|---|---|---|---|---|---|---|---|
| Explanation | If a secure component is successfully manipulated fatalities and/or multiple severe injuries can occur. | Time drift can be used for attacks. Still permanent availability is not required as internal clocks manage minimal time drift. | root is critical | stores all user information. compromising gives access to all systems using UAE | single source of truth for security status. loosing the data or manipulation makes monitoring "blind" | loss of software and config in central storage is catastrophy, if roll-back or new set-up (after incident) is required. | single source of access rights for human users and allowed assets | single source for network access | single source for network identifiers |
| Comment | | relevant to safety based on safety definition | | | | | | | |

The results are used as input to the detailed risk assessment and lay the basis for the zoning of the SuC.