EU-RAIL SYSTEM PILLAR

# Initial Risk Assessment

# Initial Risk Assessment

| | |
|---|---|
| Author(s) | SISIARIDIS Dimitrios |
| Abstract | Report of the Initial Risk Assessment |
| Config Item | System Security Risk Assessment Report |
| Document ID | Supporting Documents/SP-SEC-InitRiskAss#828046 Initial Risk Assessment |
| Classification | Public |
| Status | In Decision by Steering Group |
| Version | 1.1 |
| Revision | 828046 |
| Last Change Date | 17.02.2026 |
| Copyright | Brussels: Europe's Rail Joint Undertaking, 2026 |



## Document History

| | | |
|---|---|---|
| V1.0 05.02.2025 | Goltzsche, David (SMO RI R&D F SEC) | Approved version based on Review X.X |
| 1.0 25.09.2025 | Jorge Block | Approved version based on Review V1.0 |
| 1.1 16.02.2026 | David Goltzsche | Reviewed version including Findings from Review 1.0.9 |
| 1.0.9 23.01.2026 | Goltzsche, David (SMO RI R&D F SEC) | Reviewed version including Findings from Review 1.1 |
| 1.1 16.02.2026 | David Goltzsche | Reviewed version including Findings from Review 1.0.9 |

## 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

Approval by reviewers

| | |
|---|---|
| Type of Approval | Document Review |

Approval by approvers

| | |
|---|---|
| Type of Approval | Document Approval |

## 1 Table of Contents



## 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 | The risk occurrence comprises a single issue with politically/ legally relevant sub-aspects. Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR | Increased constraints on operations with acceptable impact on capabilities/ processes. Note: The following aspect may be relevant in the assessment:<br>- End customer service provision<br>- public supply | Country-wide and supra-regional (neighboring countries) critical reporting of sub-areas/ individuals of the company. Note: The following aspects may be | Individuals may suffer minor injuries if the system fails.. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | employment contract or other contractual relationship, personnel number. | right to personal self-determination and integrity. | | relevant when assessing reputation: Employee reputation, employer reputation, strategic target achievement at risk, loss of customers or market share / political trust. | |
| Middle | Tolerable financial damage. The financial thresholds are defined by the CISO or the CEO. | An impairment of the right to informational self-determination has a minor impact on the personal rights of the data subject. e.g. generally accessible data, address data within the scope of an employment contract or other contractual relationship, personnel number. | The occurrence of risk comprises a single issue that leads to a contractual, legal or political audit with probable consequences (e.g., penalties). Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR right to personal | Increased constraints on operations with acceptable impact on capabilities/ processes. Note: The following aspect may be relevant in the assessment: - End customer service provision - public supply | Country-wide and supra-regional (neighboring countries) critical reporting of sub-areas/ individuals of the company. Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, | If the system fails, individuals may suffer 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 |
| | | | self-determination and integrity. | | strategic target achievement at risk, loss of customers or market share / political trust. | |
| High | High financial damage. Financial thresholds are defined by the CISO | An impairment of the right to informational self-determination has a | The occurrence of risk comprises a situation/ series of situations | Extensive constraints in operative operations with high impact on capabilities/ processes or | National/ international critical reporting. The reputation of the | If the system fails, many people can 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 |
| | or the CEO. | significant impact on the personal rights of the person concerned or is a criminal offense.<br>e.g. customer or employee profiles, qualification or scoring data, wage or salary data, bank data, health data, political and | that have contractual, legal or political consequences for parts of the management.<br>Note: The following aspects may be relevant for the assessment: contractual agreements or EU-GDPR | critical facilities.<br>Note: The following aspect may be relevant in the assessment:<br>- End-user service delivery<br>- public supply | operator is at risk, market shares and new business are at risk.<br>Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer | serious injuries. As a rule, inpatient hospitalization is required. Individuals may also be killed by the failure of the system. |

| 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 |
| | | religious convictions, video surveillance and recording, telecommunication service data at the provider. | right to personal self-determination and integrity. | | reputation, strategic goal achievement at risk, customer or market share loss / political trust. | |
| Very High | Existence-threatening damage.<br>The financial threshold values are defined by | There is a high need for protection and, moreover, the processing of personal data | The occurrence of risk comprises a series of circumstances that lead | Large-scale cessation of operations.<br>Capabilities/ processes have been interrupted or | International negative reporting, image of the company damaged | 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 |
| | the CISO or the CEO. | 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.<br>For example, personal data that is subject | 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 | 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 | for the long term with all stakeholders.<br>Note: The following aspects may be relevant when assessing reputation: Employee reputation, employer reputation, strategic | |

| 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 |
| | | to professional secrecy or bank or credit card accounts at the call centre. | right to personal self-determination and integrity. | | goal achievement at risk, loss of customers or market share / 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 |
| 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 |
| 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 | 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 monitori | loss of software and config in central storage is catastrophy, if roll-back or new set-up (after incident) | single source of access rights for human users and allowed assets | single source for network access | single source for network identifiers |

| Requ / System Name | Secure Component | SCS-STS | SCS-PKI | SCS-UAS | SCS-LOG | SCS-BKP | SCS-IAM | SCS-NAC | SCS-DNS |
|---|---|---|---|---|---|---|---|---|---|
| | | manage minimal time drift. | | | ng "blind" | is required. | | | |
| 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.