# EUG
# EULYNX
# OCORA
# RCA




## (Cyber) Security Guideline

# Management Summary

One of the main objectives of the EUG, EULYNX, RCA and OCORA security workstreams is the creation of harmonized methods and processes to support railway operators and suppliers by the implementation of security procedures and methods. In this document a harmonized Security Risk Assessment for a System Design Process will be defined and presented in form of an example walkthrough. This process and guidelines are harmonized, have a consolidated approach, and are created in collaboration with EUG, EULYNX, RCA and OCORA.

This is a joint venture document from the following security workgroups:

- EULYNX/RCA Security Cluster
- OCORA TWS06 (Cyber-) Security
- (EUG) ERTMS Security Core Croup (ESCG)

# Revision history

| Version | Change Description | Initial | Date of change |
|---|---|---|---|
| 1.00 | Initial version of Security Guideline corresponding to ERORAT v1.0 | Ulrich Meier<br>Richard Poschinger<br>Max Schubert<br>Roger Metz | 30.06.2021 |
| 2.00 | General revision of the document.<br>Revision corresponding to ERORAT (Template version v2.17) | Richard Poschinger<br>Roger Metz | 20.06.2022 |
| 2.01 | Added Details regarding definition of Zones<br>Revision corresponding to ERORAT (Template version v2.28) | Ulrich Meier<br>Richard Poschinger<br>Max Schubert<br>Roger Metz | 05.09.2022 |

# Table of contents

# Table of figures



# Table of tables

# References


[1] EN 50126-1:2017 - Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[2] EN 50129:2018 - Railway Applications -Communication, signalling and processing systems -Safety related electronic systems for signalling

[3] EN 50159:2010 - Railway Applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

[4] IEC 62443 - Industrial communication networks – Network and system security

[5] ISO 27005 - Information technology — Security techniques — Information security risk management

[6] NIST 800-30 - Guide for Conducting Risk Assessments (July 2002 and September 2012)

[7] NIST 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations

[8] TS 50701 - Railway Application – Cybersecurity

[9] VDE V 0831-104: 2015-10 - Elektrische Bahn-Signalanlagen Teil 104: Leitfaden für die IT-Sicherheit auf Grundlage IEC 62443

# 1 Introduction

## 1.1 Release information

(Cyber) Security Guideline

Version: 2.01

Publication date: 05.09.2022

## 1.2 Imprint

**Publisher:**

ERTMS Users Group



**Authors:**

- Meier, Ulrich (ulrich.meier@sbb.ch)
- Metz, Roger (roger.metz@incyde.com)
- Poschinger, Richard (richard.poschinger@incyde.com)
- Schubert, Max (max.schubert@incyde.com)

## 1.3 Purpose of the document

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 EUG, RCA, EULYNX and OCORA.

Three railway-initiated initiatives (EULYNX, RCA and OCORA) drive the harmonization of requirements for modular CCS architecture (see Figure 1).

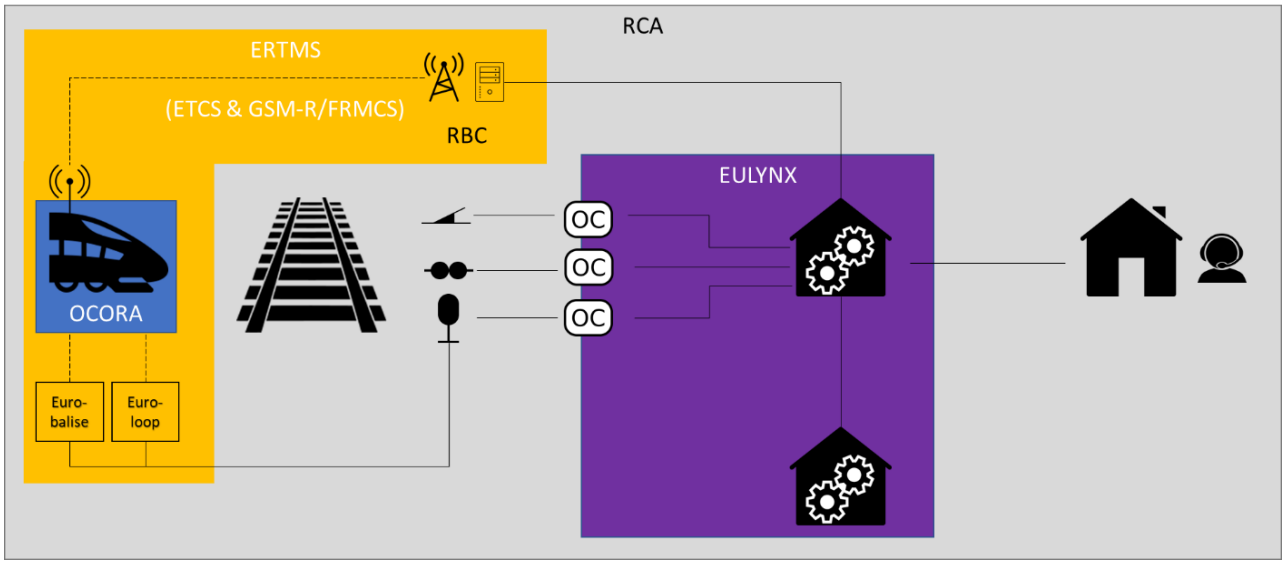


Figure 1: Relations of EULYNX, RCA and OCORA

This document is addressed to experts in the railway security domain and any other person, interested in security engineering processes.

# 2 Guideline Definitions

## 2.1 Guideline Approach

The EN 50126 [1] understands “security” as resilience of the railway system to vandalism, malevolence, and intentionally harmful human behaviour. As the standard does not introduce a dedicated topic “security”, as it does with “safety” or “reliability, availability and maintainability”, it is acceptable by the EN 50126 [1], to apply the security engineering processes proven in other industries, e.g. IEC 62443 [4]. TS 50701 [8] documents the interaction of both worlds. As a result, the detailed steps of a security engineering process are de-coupled from the V-model of the EN 50126 [1]. This means that the security engineering process must provide relevant artefacts to the phases of the V-model matching the required level of detail for each phase. This results in artefacts, e.g., the cyber security case, are gaining granularity during the EN 50126 [1] phases.

The security engineering process will cover the system under consideration and its interfaces and relations to surrounding systems. These systems may be in similar technology or maturity level as the system under consideration. It is also possible that interfaces to legacy systems need to be considered.

Both, the decoupling of security solution development and the vehicle/infrastructure specific situation of surrounding (incl. legacy) systems lead to the conclusion, that the system integrator must be aware of its key role. The Integrator must coordinate and manage during the development process (phase 1 to 10). During life cycle phase 11 (operation), the operating organization must take over this role (e.g., in a life-cycle manager role or in an operation management organization leading change, configuration, or maintenance processes.)

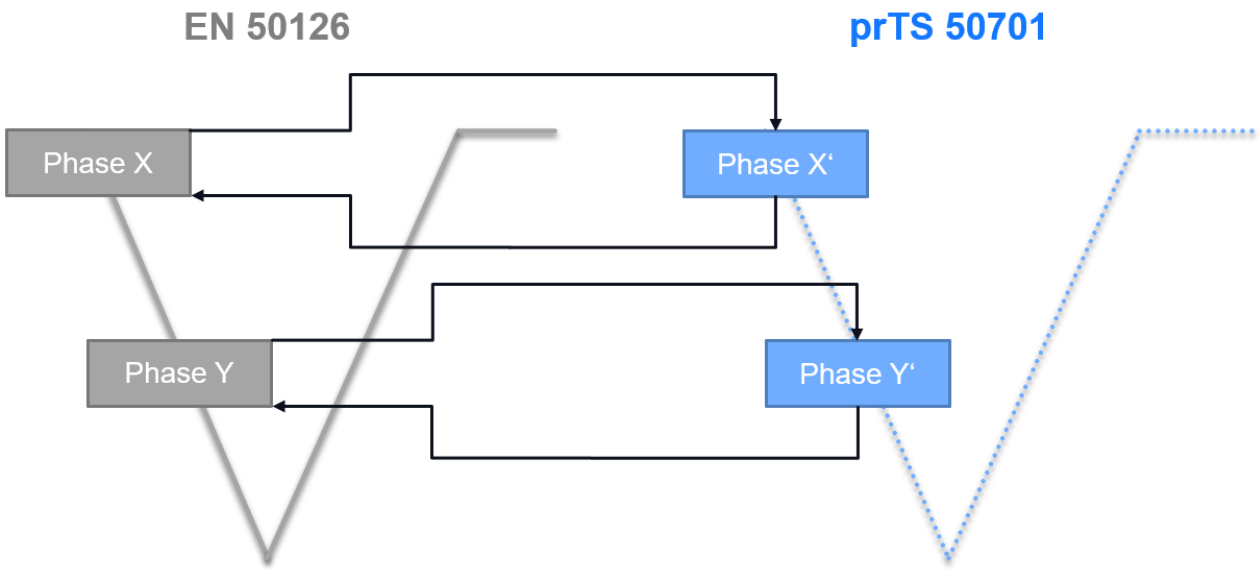


Figure 2: Process Interaction

Security solutions are not subject to assessment in contrast to railway solutions, which are developed according to EN 50126 [1]. Therefore, the process of security engineering can be run through separately. However, synchronization is necessary to ensure the coordinated transfer of input and output. Each phase of an EN 50126 [1] project has an equivalent in the security engineering process and needs to be provided with necessary information to perform the planned activities.

This synchronisation is also necessary to fulfil the Guideline 4 from the guiding principles for security-safety conflicts according to TS 50701 [8]. The result of each phase on the security side must be verified. This is a cyber security verification activity, which is not related to any safety guidelines or standards. This lays the base for the validation and cyber security system acceptance.

The phases of the security engineering process should be mapped to the equivalent CENELEC phases to ensure the verification- and/or validation tasks are also performed for the results and outputs from this process. It is up to the railway operator to implement this mapping. The responsibility of integration of the security solution lies also with the railway operator. In addition to a secure operator concept, a secure solution also includes a secure system integration and secure solution implementation according to IEC 62443 [4] and TS 50701 [8]. Every element must be considered with the knowledge that the achieved level of security degrades over time or in case of unforeseeable events. The following table shows this synchronisation of input artefacts, risk management activities and the related output artefacts as an example.

| | CENELEC Phase | | | | |
|---|---|---|---|---|---|
| | 1. Concept | 2. System Definition and operational Context | 3. Risk Analysis and evaluation | 4. Specification of System Requirements | 5. Architecture and Apportionment of System Requirements |
| **Security related Input:** | Purpose and Scope<br>Applicable security standards<br>Operational environment incl. exciting controls | System boundaries<br>Initial System Architecture<br>List of functions and interfaces<br>Logical and physical network plans | Functional requirements (linked to essential functions) | Preliminary documentation | System architecture breakdown to components |
| **Security related Activities: Risk Management** | CIA (Confidentiality, Integrity, Availability) Analysis & Classification<br>Challenges & Approaches | Definition of threat landscape<br>Impact Analysis<br>Definition of risk acceptance criteria<br>Risk Matrix | Zone based Risk Analysis<br>Refinement of initial impact assessment in the Threat Log | Detailed Risk Analysis<br>Definition of requirements<br>Definition of application conditions | Component based risk analysis<br>Update of countermeasures |
| **Security related Output:** | Project Security Management Plan | Impact analysis<br>Zones and Conduits | Threat context<br>Initial Threat Log<br>Potential updates (like zones or network plans) | Zone based security requirements specification<br>Security related application conditions | Component based security requirements specification<br>Security related application conditions |

Table 1: Mapping Security model to EN 50126 Phase Model - Example

## 2.2 Process Evaluation

For the creation of a complete and harmonised process the first step was the comparison and evaluation of the most important security standards in terms of the Security Risk Assessment for System Design. Figure 3 shows the currently available processes.


Figure 3: Security Risk Assessment for System Design Process Comparison

An evaluation was carried out to be able to suggest an optimal process.

The main evaluation aspects were:

- Relevance for operational technology (railway context)
- Acceptance in the field of industries and probably also from appraiser / federal organizations
- Usability
- Applicability
- Level of detail given by the standard
- No more complexity than needed

ISO 27005 [5]:

The ISO-standard is focussing on security risk management for organisations in the context of the ISO 27000 [5] standard and does not focus on operational technology or applications. That is why it is not widely used in the industry field whilst it is referenced as an umbrella process. For the applicability, a more detailed focus is needed.

NIST 800-30 [6]:

The NIST standard is an application focused standard that could be used for operational technology and is widely recognized. On the other side, it is not related to any European standard, so the acceptance within European experts, regulatory bodies and governmental organizations could be negatively affected.

IEC 62443 [4]:

This standard is focussing on operational technology, touching the business and risk management side as well as the technological part. Furthermore, the standard is widely used in the European industry and accepted by appraisers and federal organizations.

TS 50701 [8]:

This technology standard and technical specification are mainly based on IEC 62443 [4] and references also NIST 800-30 [6]. With that it combines the technological standards of both and completes the processes with railway specific content to allow an easier reference for the railway managers and railway operators.

VDE V 0831-104 [9]:

This German (pre-) standard is referenced and based on IEC 62443 [4], as it was developed similarly to the TS 50701 [8] and its adds one very useful option to ensure applicability, which is the possibility to adjust the required security levels (SL) depending on railway specific factors like the accessibility of the location. Due to its state as a national pre standard for Germany, it is not widely used.

### 2.2.1 Security Risk Assessment Structure

As an additional result from the Process Evaluation a main structure is given for the security process:

1 Architectural Design with Zone Concept
2 Threat Analysis
3 Risk Analysis (structural analysis)
4 Measures
5 Integration / Security Architecture / Specification

### 2.2.2 Security Risk Assessment Approach

There are two approaches to define the security measures based on a risk analysis. Following the standards, NIST [6] [7], IEC 62443 [4], ISO 27005 [5] a static analysis is done. That means that a strict process is followed that respects the systems, attacker types, standardized measures, and mitigation strategies, not considering the likeliness of an attack. The second approach follows the function of the automated system and tries to find the right measures by foreseeing the possible attacker strategies. The following table shows the advantages and disadvantages:

| | Static | Functional |
|---|---|---|
| Advantage | - Standards based<br>- audit capability<br>- proven measure<br>- easy to commonly agree on<br>- can be set into relation of process from EN 50126 [1] / Safety approach | - taking the actual function of the system into relation<br>- can be more efficient from the cost point of view, when applied with a lot of experience and courage |
| Disadvantage | - no quantification of likeliness of an event<br>- may be more “expensive” than the functional approach | - no back-up by a standard<br>- risk of forgetting attack methods (forget to secure the hidden champion)<br>- not one by one connectable to safety (EN 50126 [1])<br>- no basis for continuous improvement process |

Table 2: Advantages and disadvantages of static and functional approaches

After evaluating the table above, it is highly recommended to follow the static risk analysis. The functional aspect can be filled in for the risk reducing factors and when defining the actual measures for risk mitigation.

That is why this document follows the above-mentioned norms.

The functional approach can be added in a second step after a time of experience to start a continuous improvement process.

# 3 Process Definition

In this chapter the whole process for the risk assessment is described, which is based on the decision of chapter 2.2 to use TS 50701 [8] as the basic standard.

In this chapter the process is defined, the process itself is presented with all steps and each step is described in the following chapters.

Further, the process can be implemented using ERORAT (EULYNX RCA OCORA Risk Assessment Tool). This Excel file is meant to be the risk assessment tool for EULYNX, EUG, RCA and OCORA. ERORAT is not provided publicly and available to members of the participating organizations.

The results documented in ERORAT can be adapter to the IM/RU implementation to respect individual needs and legacy systems.

ERORAT leads you through the described process step by step. The steps are synchronized between this document and ERORAT. The references to ERORAT are always printed in blue coloured text.

The following process steps were defined, based on IEC 62443 [4], TS 50701 [8] and best practice:

**Covered in the Concept:**

1. Define system under consideration (SUC) (according to TS 50701 [8] and IEC 62443 [4]) following the architecture.
2. Initial zoning concept based on reduced risk assessment or assessment of protection requirements.
3. Define attacker types (generic)
    a. Overall definition
    b. Add attacker capabilities, motivation, and resources
    c. Evaluation and exclusion

**Per Zone in ERORAT-Tool:**

4. Define threats e.g., from the BSI catalogue, supplemented and sorting of threats into the Foundational Requirements
5. Definition of SL-T
    a. Definition of maximum attacker type
    b. Definition of the initial iSL per threat in FR based on the Impact
    c. Asses reducing factors and reduce iSL -> SL-T per threat
    d. Evaluation of the SL Vector
6. Now the measures according to IEC 62443 [4] are preselected: Select SR based on the SL-Vector
7. Apply the risk assessment
    a. Perform initial risk assessment
    b. Select SRs as mitigating measures if necessary
    c. Perform risk assessment including selected SRs
    d. Select additional mitigating measures if necessary
    e. Perform final risk assessment
    f. Check if resulting risk can be accepted
        i. If yes: Provide reason for accepting final risk (if necessary)
        ii. If no: Check if additional measures are necessary and start from step 7.b.
8. Define explanations for unused SRs and perform completeness check

In the following the process is inserted into a flow chart to visualize it.

The blue part of the process can be documented using ERORAT, where a model solution is displayed already.

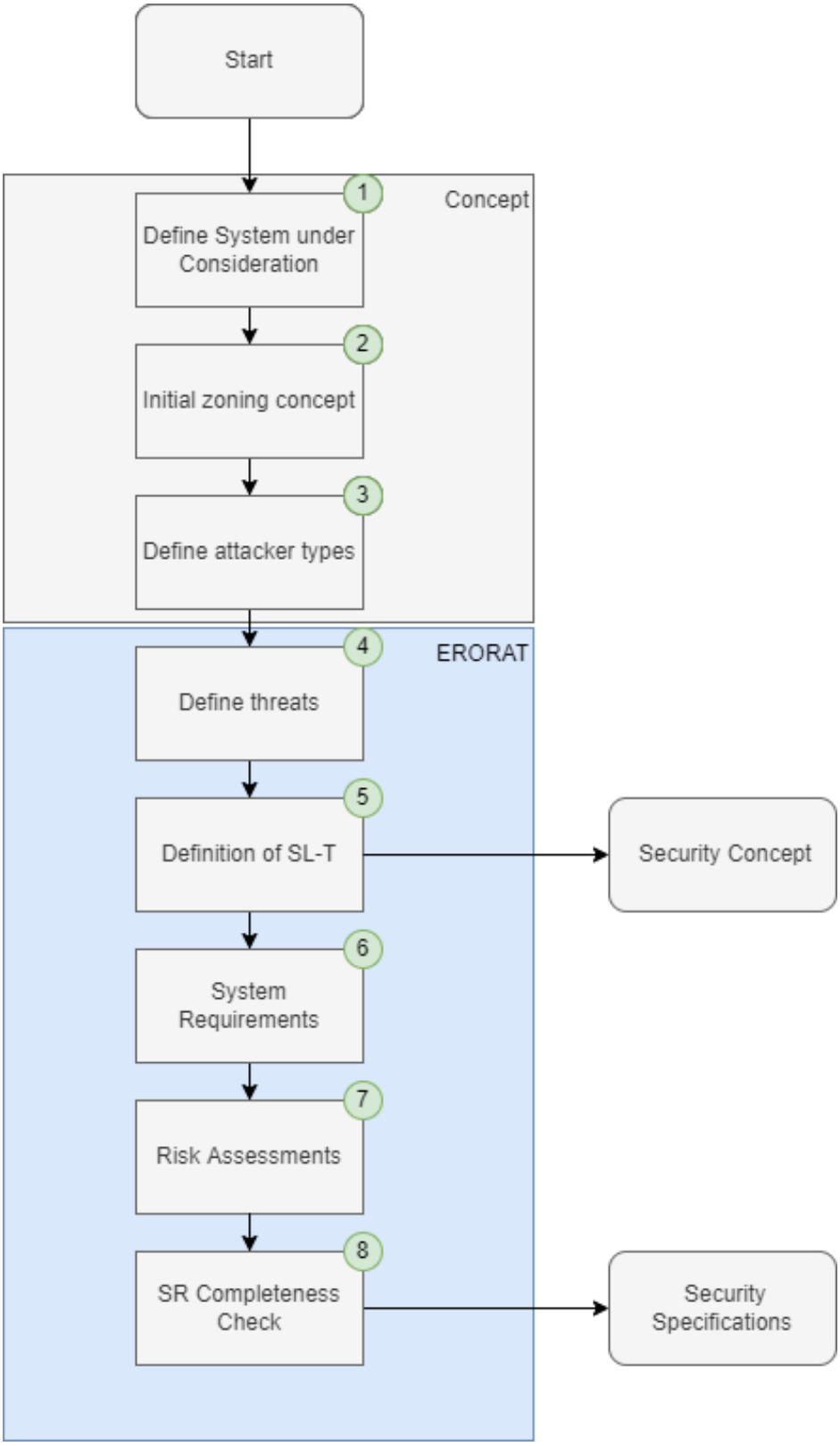


Figure 4: Security Process

All these steps are described in detailed in the following subchapters.

## 3.1 System under Consideration

Description based on standards including the following information:

- Scope, context, and purpose of the SuC
- Presentation of the environment of the SuC
- System boundaries
- Functionalities provided by the SuC
- Interfaces (external and internal)
- Identification of the RAMSS requirements from past experiences
- Presentation of the RAMSS policy used
- Presentation of the safety and security legislation
- List of assumptions and justifications for the SuC (Example according to TS 50701 [8])

## 3.2 Definition of Zoning for Architecture

The system definition or system under consideration is the basis for defining zones and conduits. Zones defined in this process are explicitly not equal to physical network zones.

The aim of defining zones and conduits is to group systems or components that have the same requirements from the security point of view, due to similar threats and possible impacts. Therefore, an initial reduced risk assessment is needed. As an alternative the zones can be analysed based on the protection requirements.

The zone concept follows TS 50701 [8]. The integration and application of the zone model is highly depending on the IM/RU system under consideration, also due to legacy systems or processes.

The following rules are defined and applied:

**Zones** are:

- components and systems with same or similar protection requirements
- components and systems with similar operational and functional aspects
- at one location

**Conduits** connect:

- zones with different protection requirements
- zones with same protection requirements in different locations

## 3.3 Define Attacker Types and determine preliminary Security Levels

In this step it is considered from whom or from what the threat emanates.

The IEC 62443 [4] definition of the term *attack* is an assault on a system that derives from an intelligent threat.

The attacker can be a person or a group/organisation.

The determination of the severity of a threat event follows the system of the IEC 62443 [4], referenced in TS 50701 [8], after which the type of attacker and its possibilities are defined.

In this step, attacker types are identified that could cause certain threats.

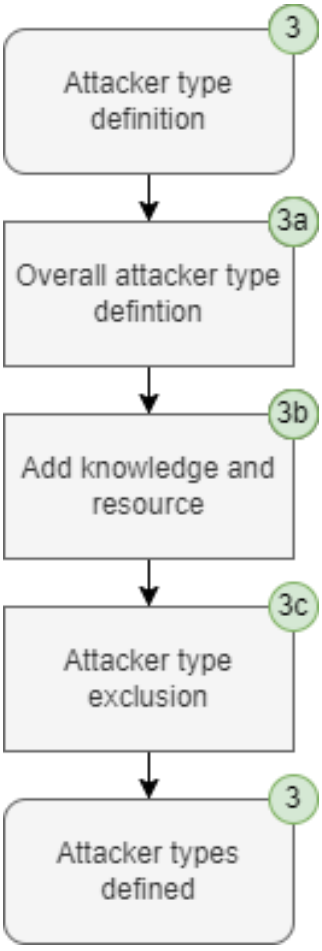


Figure 5: Attacker Definition

- **3a: Overall Attacker Type Definition**

The attacker definition is the basis to allow classification of the threats and to define a likelihood. Intentional targeted attackers can be split into several categories. These are persons or organizations who intentionally would like to damage the SuC. Targeted attacks are the focus of the analysis. Examples for attacker types can be found in Appendix A.

- **3b: Add Knowledge and Resources**

In this step the knowledge and resources are added to each attacker type. The range of values for both categories is defined in Table 3.

- **3c: Attacker Type Exclusion**

The maximum values of the attacker type taken into consideration in the assessment is used to define the maximum SL-T (SL-T_Max). The SL-T_Max represents the upper bound of the SL-T (Security Level Target) which is used to derive SRs.

For this purpose, the following table from IEC 62443 [4] is used.

| SL-T_Max | | Resources | | |
|---|---|---|---|---|
| | | 2 Low | 3 Moderate | 4 Extended |
| Know-ledge | 2 General | 2 | 3 | 4 |
| | 3 Specific | 3 | 3 | 4 |
| | 4 Extended | 3 | 4 | 4 |

Table 3: Attacker Knowledge and Resources

Theoretically every possible attacker type can occur. To get more details on attacker types, threat analysis from governmental organization can be considered.

ENISA is supporting the EU Member States since 2012 to develop, implement and evaluate their National Cyber Security Strategies (NCSS). Since 2017, all EU Member States have published their own NCSS (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map).

Some attackers might be excluded as they are not expected to target the SuC. For example, state attackers might not be considered to target the operator of a small railway line which is not categorized as critical infrastructure.

As the reason for excluding some attacker types may change over time or due to a change in the threat landscape, it is mandatory to periodically re-check the exclusion or be prepared to mitigate the attacker type within reasonable timing and effort. This could be done using extended defence in depth, monitoring or resiliency in mission critical processes or being prepared for degraded operation.

The set of all attacker types without excluded attackers results in maximum values for resource and knowledge. These values define the SL-T_Max based on the definition in Table 3.

The SL-T Max is added to ERORAT.

Tab “SL-T”, Section “Assumption on attacker type - 3c”

## 3.4 Threats Definition

The threat definition is separated into two major steps, which are described in the following two subchapters.

### 3.4.1 Threat Catalogue

The risk assessment as well as the definition of the SL-T is based on the threats defined in ERORAT. Different threat catalogues can be used.

These threat landscapes are available from the following institutions UIC, CERT-EU, ENISA, BSI. The threat catalogue shall be chosen based on the following criteria:

- Completeness:
  The threat catalogue should cover all relevant aspects of the domain (ERTMS, CCS etc.). It is necessary to define if environmental threats and physical attacks shall be considered as well. If these aspects are excluded, it must be stated in the security concept.
- Number of Threats:
  The grade of details based on the definition of different threats needs to be sufficient to perform a detailed analysis. However, the number of threats must be limited to a minimum which is feasible in the analysis phase.
- Sufficient Definition of Threats:
  Each threat must be described in detail and unambiguous. The description of a threat must be explicit, so that a threat can is not mixed up with another threats.

As existing threat catalogues might not take all relevant aspects into account, (e.g., railway specific threats). Hence additional threats can be defined and added to the ERORAT. Furthermore, threats of an existing catalogue can be split up or aggregated according to the requirements of the assessment.

Tab “Threats_SL”, Section “4a (Threat Catalogue)”

### 3.4.2 Threat Mapping to the foundational Requirements

In this step each threat (based on the catalogue) must be mapped to the foundational requirements (FR) from IEC 62443 [4]. This is to ensure conformity with TS 50701 [8] that refers to IEC 62443 [4] concerning the actual security measures.

Based on this mapping the SL-T is defined and relevant SRs (IEC 62243 [4]) are selected.

There are seven Foundational Requirements (FR) in place, the identified threats need to be sorted to:

1. Identification and authentication (IAC - Identification and authentication control)
   In this FR threats are assigned, which lead to unauthorized access and/or access to the system or system components.
2. Usage control and monitoring, authorization (UC - Use control)
   In this FR threats are classified, which lead to an unauthorized use of the system due to missing or dysfunctional use control.
3. System integrity (SI - System integrity)
   In this FR, threats are assigned related to manipulation of data or components.
4. Confidentiality (DC - Data confidentiality)
   In this FR, threats are assigned that are related to unauthorized access to, or disclosure of sensitive data or information.
5. Restricted data flow (RDF - Restricted data flow)
   In this FR, threats are assigned that lead to inadmissible managed data flows.
6. Reacting to events in good time (TRE - Timely response to events)
   Threats that delay or prevent the response to security relevant events are assigned to this FR.
7. Availability of resources (RA - Resource availability)
   Threats that interrupts your resource supply, which is required for continuous operation, e.g., energy supply.

Tab “Threats_SL”, Section “4b (FR)”

## 3.5 Definition of SL-T

The definition of the target SL (SL-T) is necessary to have a documented basis for choosing the required measures to ensure security for the system. For this purpose, a formal process is applied.

The result is the final target Security Level for each zone, SL-T. Tab “SL-T”, Section “SL-Vector – 5f”

The whole process is displayed in Figure 6, whilst the sub steps are explained beneath.

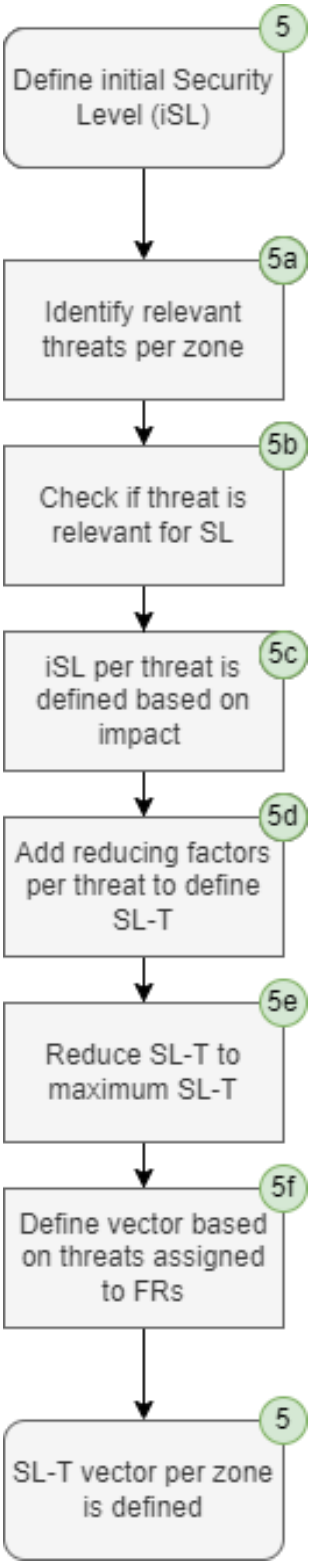


Figure 6: Define initial Security Level Subprocess

- **5a: Identify relevant threats per zone**

After the threats have been sorted to the FR in the process step number 4 (see Chapter 3.4.2), the relevant threats for the zone must be identified.

ERORAT uses a table to mark which threat is relevant for the zone.

If the threat is not relevant for this zone: Provide a reason and explanation why the threat is not considered to be relevant.

Tab “Threats_SL”, Section “5a – Relevance”

Tab “Threats_SL”, Section “5a – Explanation / Reason why not relevant”

- **5b: Check if the threat is relevant for SL calculation**

IEC 62443 describes the applicability of the standard: “Notably, the causes of these risks are related to cyber security threats as opposed to other factors such as fire, flood, vandalism and safety hazards threats.” [4]

As the selected threat catalogue might contain additional threats (not included in IEC 62443 definition), these threats should not be included in the SL calculation. Otherwise, the SL could be higher than required.

Even if the value is excluded from the calculation for a certain threat, this threat can still be mitigated using an SR.

Tab “Threats_SL”, Section “5b – Include into SL-T calculation“

- **5c: iSL per threat is defined based on impact**

The iSL is based on the threat which is also used as input value for the initial risk assessment.

The impact is rated according to the definition of TS 50701 [8].

Tab “Threats_SL”, Section “5c – Impact”

Tab “Threats_SL”, Section “5c – iSL-T”

- **5d: Add reducing factor per threat to define SL-T**

LOC = 1 if the zone cannot be attacked remotely and therefore an attacker must physically penetrate the zone to carry out an attack on railway premises or within railway buildings.

LOC = 0 otherwise.

$iSL_{-T} = iSL - LOC$

Tab “Threats_SL”, Section “5d - Reducing Factors”

- **5e: Reduce SL-T to maximum SL-T**

The SL-T has to be reduced (if necessary) to the maximum SL-T previously defined based on the attacker type exclusions.

Tab “Threats_SL”, Section “5e – SL-T”

- **5f: Define vector based on threats assigned to FRs**

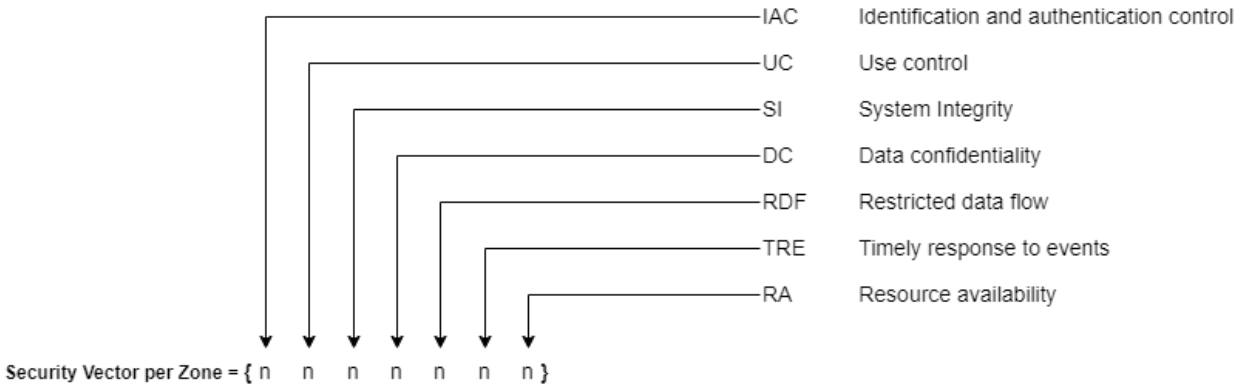


Figure 7: Security Vector

The SL-T vector (as defined in Figure 7) is defined for every FR based on the maximum values and the assignment of threats to FR. It is illustrated by the following example.

*SL-T(FR) = max (SL-T of all Threats assigned to this FR)*

A resulting vector could look like this:

*SL-T vector = {1,2,3,3,2,1,3}*

This SL-T vector can be transformed into an universal SL-T value by calculating

*SL-T = max (SL-T vector)*

In this example the SL-T value is:

*SL-T = max (1,2,**3**,**3**,2,1,**3**) = **3***

Tab “SL-T”, Section “SL-Vector – 5f”

After the above explained process steps (5a – 5f) the SL-T vector per zone is defined.

## 3.6 System Requirements

Based on the SL-T vector which has been defined in process step 5, the relevant SRs can be selected. This task is performed to prepare the SR selection as mitigating measures in the risk assessment (step 7).

Depending on the SR-T for each FR (part of the SL-T vector) the System Requirements are selected.

The following example will explain this procedure:

| | | |
|---|---|---|
| SR 1.2 RE 1 | IAC | 3 |

SR 1.2 RE 1 is assigned to IAC (FR) and its lowest SL-T is 3.

Hence, it is only relevant for the next processual steps if the SL-T of IAC >= 3.

In the ERORAT template this step is automatically done in the Tab “SL-T”, Section “Assumption on attacker type - 3”. The update filter function must be used to see the relevant SRs after a change in the SL definition.

## 3.7 Risk Assessment

In step 7 the actual risk assessment is carried out and the necessary measures are identified based on the analysis of risks for the considered zone.

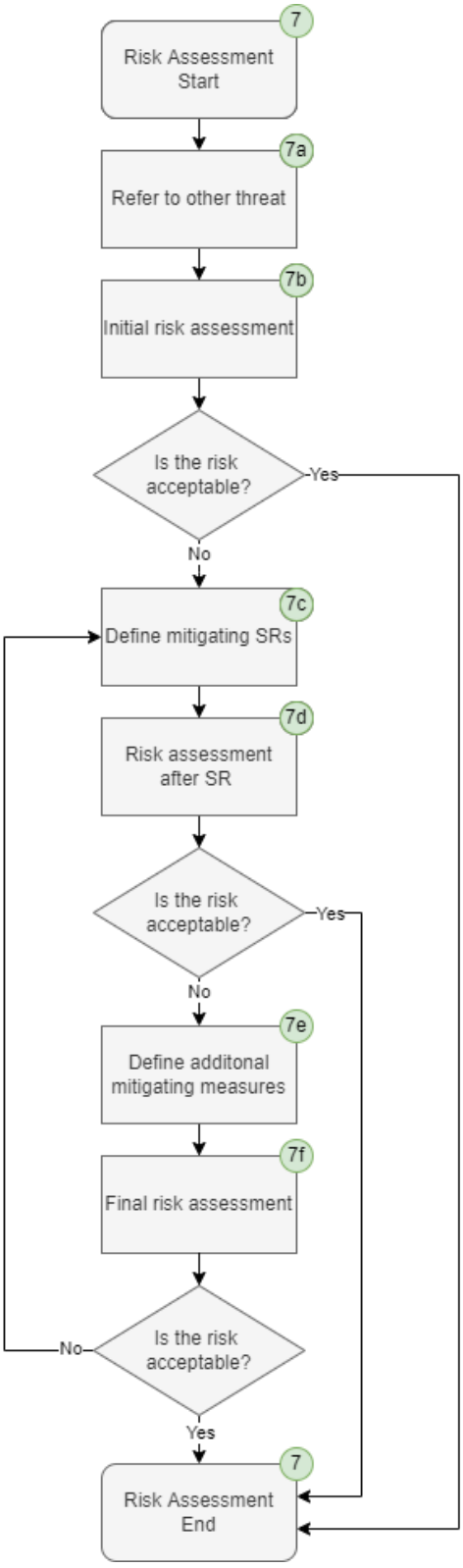


Figure 8: Risk Assessment

By applying this process, the following goals are achieved:

1. Fully performed security evaluation process following TS 50701 [8]
2. Measures applied following IEC 62443 [4]
3. Definition of risk delta and risk acceptance
4. System requirement for security

Additional SRs which are not marked as relevant can be applied if it is necessary according to the risk delta.

### 3.7.1 Definition of the target risk

The target risk must be defined, which represents an acceptable risk for the institution. All risks matching this target risk (or lower risks) can directly be accepted without any reason.

Default target risk = Low

Tab “SL-T”, Section “Risk - 6”

### 3.7.2 Risk Assessment Process

The following steps are used to perform the risk assessment (as shown in Figure 8):

a) Refer to other threat

If the threat is relevant but the results of all assessment steps are expected to be similar to another threat, it is possible to refer to this threat. Additionally, a reason for referring to another threat can be provided.

Tab “Risk_evaluation”, Section “7a”

b) Initial risk assessment

The initial risk assessment is carried out without considering any measures. Thus, it is based on the systems current architecture.

The risk is evaluated according to Chapter 3.7.3.

If the risk is accepted according to Chapter 3.7.4 the process for this threat is finished.

Tab “Risk_evaluation”, Section “7b”

c) Define mitigating SRs

SRs can be selected as mitigating measures based on the identified SRs relevant for this zone in step 6.

Tab “Risk_evaluation”, Section “7c”

d) Risk assessment after SR

This risk assessment is carried out considering that the previously selected SRs have been applied to the system.

The risk is evaluated according to Chapter 3.7.3.

If the risk is accepted according to Chapter 3.7.4 the process for this threat is finished.

Tab “Risk_evaluation”, Section “7d”

e) Define additional mitigating measures

Additional mitigating measures (including measures from IEC 62443-2-1) or more detailed variants of the previously selected SRs can be described here.

Tab “Risk_evaluation”, Section “7e”

f) Final risk assessment

The final risk assessment is carried out considering that all necessary measures have been defined and applied to the system.

The risk is evaluated according to Chapter 3.7.3.

If the risk is not accepted according to Chapter 3.7.4 the process needs to be continued at c).

Tab “Risk_evaluation”, Section “7f”

### 3.7.3 Evaluation of the actual risk by using the following steps and calculations

These steps are repeated in every risk assessment:

The risk is evaluated before measures have been applied, after IEC 62443 [4] measures have been applied and after additional compensating measures have been applied. Thus, the risk must be evaluated in three steps. If no measures are applied after a risk evaluation the risk does not have to be re-evaluated.

- **Evaluation of the Exposure of the system**

  This is performed by using the standardised exposure categories from 1 to 3, based on TS 50701 [8] (Definition: Tab “Likelihood”). The result of this evaluation, which is usually performed by a group of experts, is documented. Tab “Risk_evaluation “, Column “Exposure”

- **Evaluation of the Vulnerability of the system**

  This is performed by using the standardised vulnerability categories from 1 to 3, based on TS 50701 [8] (Definition: Tab “Likelihood”). The result of this evaluation, which is usually performed by a group of experts, is documented. Tab “Risk_evaluation “, Column “Vulnerability”

- **Evaluation of the Impact of a failure or manipulation of the system**

  This is performed by using the standardised impact categories from D to A, based on TS 50701 [8] (Tab “Impact”). The result of this evaluation, which is usually performed by a group of experts, is documented. Tab “Risk_evaluation“, Column “Impact”

  The result of exposure and vulnerability is calculated to a likelihood in the categories 1-5 following TS 50701 [8]. Tab “Risk_evaluation“, Column Likelihood”

  In the end the combination of likelihood and threats results in a risk (Definition: Tab “Risk”).

  Tab “Risk_evaluation“, Column “Actual Risk”

### 3.7.4 Evaluation of risk delta

This step is done after every risk assessment:

- **Evaluate risk delta**

  **If the risk delta is > 1**, compensating measures must be in place and documented. This must be done until the risk delta is <= 1.

  **If the risk delta is 1**, compensating measures should be in place and documented to reduce the risk delta to 0. It Is possible to accept a risk delta of 1 for among others the following reasons:

  - Technical restrictions
  - Restrictions in terms of financial and temporal feasibility
  - Feasible measure has a negative impact on operation

  Reasons must be given why no applicable measures were found, which would reduce the risk to delta = 0.

  **If the risk delta is 0,** no additional measures must be considered.

## 3.8 SR Completeness Check

In the previous steps SRs were filtered based on the SL defined in the ERORAT tool. Some of these SRs might have been selected during the risk assessment while others could not be used. To meet the regulatory requirements, it is necessary to assure that all necessary SRs are implemented. The SR must not be implemented

- if the SR cannot be applied to the zone (e.g., SR for radio connections if not radio connection exists)

  OR

- if the SR is not required as proved by the risk assessment.

To assure that all required SRs have been selected, the ERORAT tool shows SRs which are relevant. Furthermore, the table shows which SRs are selected. Thus, it is possible to check which relevant SRs are currently not selected to either fix the risk evaluation or detect unnecessary SRs. If the SR is finally categorized as not relevant a reason can be provided, why this SR is or cannot be used.

# Appendix A

**A.Int.TerrorOrg**

These organizations are made up of radicalized persons, who are drawn from political or religious motives (right-wing, left-wing, Islamism, Christianism, etc.) carry out targeted attacks and can have extensive possibilities if they have appropriate supporters. Attacks on rail transport may be carried out by terrorism, which is aimed at unsettling the population.

K4

R4

iSL4

**A.Int.CriminalOrg**

A criminal organization consists of persons who have made it their goal to achieve financial goals through illegal actions such as fraud or extortion. They range from small gangs to large, organized crime organisations (e.g., the mafia). The primary goal is to obtain money. Actions that are designed to simply causing damage are rare for this type of attacker.

K3

R3

iSL3

**A.Int.GovOrg**

These attackers are organized by the state and therefore have both, very high financial resources and enormous technical capabilities and skills. Governmental criminal organization can have different goals. They can either try to make profit using e.g., ransomware or get involved in cyber wars against other countries.

K4

R4

iSL4

**A.Int.Comp**

There are different CCS supplier companies that compete. It is therefore conceivable that an CCS system supplier could disrupt or manipulate the systems of the competitor, to damage the image of the competitor. It is not assumed that one railway operator attacks another one.

K4

R3

iSL4

**A.Int.Activist**

Activists are primarily politically motivated attackers who oppose political parties, who want to enforce their interests. The railway undertaker or the Rail transport can become the focus of activists, e.g., the transport of Castor containers case.

It is assumed that these are external persons or organizations who do not have detailed information on the internal structure of the railway. Availability attacks (achieving a blockade) are conceivable, causing security-critical situations (accidents) in which persons are injured do not correspond to their motivation.

K2

R3

iSL3

**A.Int.Hacker**

A hacker is generally a technically skilled computer user who has a large knowledge of current attack techniques. Black-hat hackers are using weaknesses identified in the reconnaissance phase to enrich themselves financially.

K3

R2

iSL3

**A.Int.Internal**

Internal attackers are persons who, as employees or suppliers, have internal knowledge and potentially have access to IT-systems and use them to carry out deliberately damaging actions, such as sabotage, betrayal of secrets or infidelity. Internal attackers must be treated in a different way, since the standard approach does not apply, since part of the security measures, following the IEC 62443 [4] are not valid anymore, considering that access can be easily granted to internal attackers.

K4

R2

iSL3