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 Group (ESCG)

Revision history

Version	Change Description	Initial	Date of change
1.00	Initial version of Security Guideline corresponding to ERORAT v1.0	Ulrich Meier Richard Poschinger Max Schubert Roger Metz	30.06.2021
2.00	General revision of the document. Revision corresponding to ERORAT (Template version v2.17)	Richard Poschinger Roger Metz	20.06.2022
2.01	Added Details regarding definition of ones. Revision corresponding to ERORAT (Template version v2.28)	Ulrich Meier Richard Poschinger Max Schubert Roger Metz	05.09.2022
2.02	Added additional details regarding the link to ERORAT and removed outdated content. Revision corresponding to ERORAT (Template version v2.33)	Ulrich Meier Richard Poschinger Max Schubert	07.06.2023
2.03	Minor improvements and error corrections Optimized Details regarding zones	Juhana Yrjölä Richard Poschinger Roger Metz	22.11.2023
3.00	Revision corresponding to ERORAT (Template version v3.01)	Richard Poschinger	21.11.2024

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

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

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

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

[6] TS 50701 - Railway Application – Cybersecurity

[7] 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: 3.00

Publication date: 21.11.2024

1.2 Imprint

Publisher:

ERTMS Users Group

Authors:

- Yrjölä, Juhana (juhana.yrjola@fintraffic.fi)
- 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).

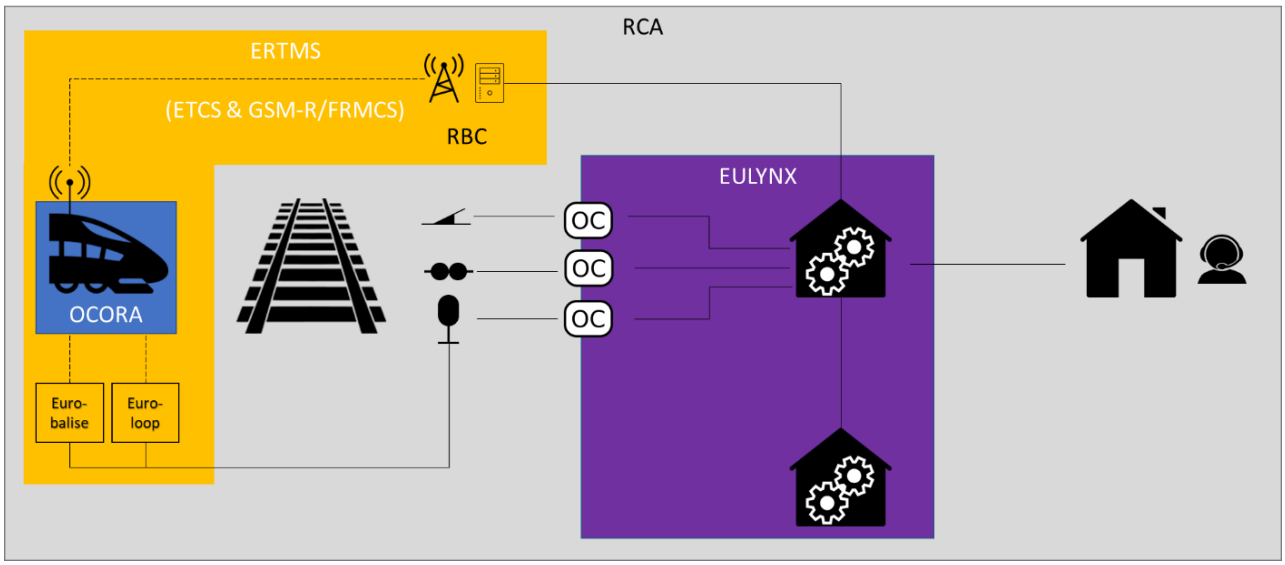

Figure 1: Relations of EULYNX, RCA and OCORA

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 [2]. TS 50701 [6] 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.)

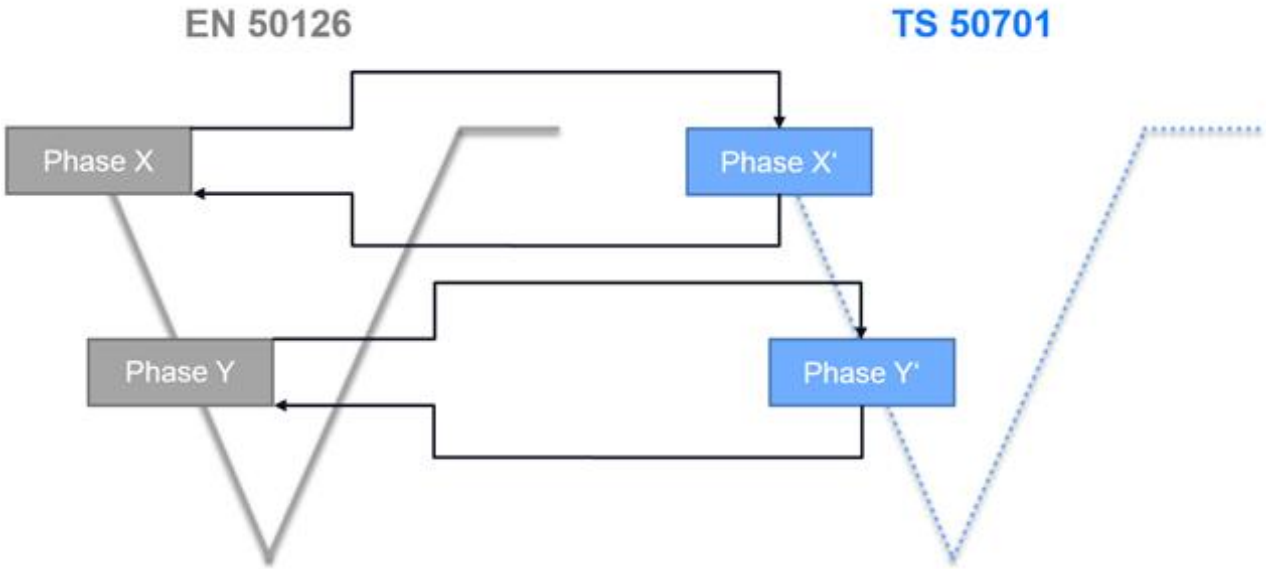

Figure 2: Process Interaction

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 [6]. 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 [2] and TS 50701 [6]. 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 Applicable security standards Operational environment incl. exciting controls	System boundaries Initial System Architecture List of functions and interfaces 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 Challenges & Approaches	Definition of threat landscape Impact Analysis Definition of risk acceptance criteria Risk Matrix	Security Zone based Risk Analysis Refinement of initial impact assessment in the Threat Log	Detailed Risk Analysis Definition of requirements Definition of application conditions	Component based risk analysis Update of countermeasures
Security related Output:	Project Security Management Plan	Impact analysis Security Zones and Conduits	Threat context Initial Threat Log Potential updates (like zones or network plans)	Security Zone based security requirements specification Security related application conditions	Component based security requirements specification 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 [3]:

The ISO-standard is focussing on security risk management for organisations in the context of the ISO 27000 [3] 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 [4]:

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 [2]:

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 [6]:

This technology standard and technical specification are mainly based on IEC 62443 [2] and references also NIST 800-30 [4]. 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 [7]:

This German (pre-) standard is referenced and based on IEC 62443 [2], as it was developed similarly to the TS 50701 [6] 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.

2.3 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 Security Zone Concept
2 Threat Analysis
3 Risk Analysis (structural analysis)
4 Measures
5 Integration / Security Architecture / Specification

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 [6] 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 EUG 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 [2], TS 50701 [6] and best practice:

Covered in the Concept:

1 Define system under consideration (SuC) (according to TS 50701 [6] and IEC 62443 [2]) following the architecture.

2 Initial security zoning concept (security zones and conduit drawing) based on reduced risk assessment or assessment of protection requirements.

Per Security Zone in ERORAT-Tool:

3 Define threats e.g., from the BSI catalogue, supplemented and sorting of threats into the Foundational Requirements

4 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. Assess reducing factors and reduce iSL -> SL-T per threat

   d. Evaluation of the SL Vector

5 Now the measures according to IEC 62443 [2] are preselected: Select SR based on the SL-Vector

6 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.

7 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.

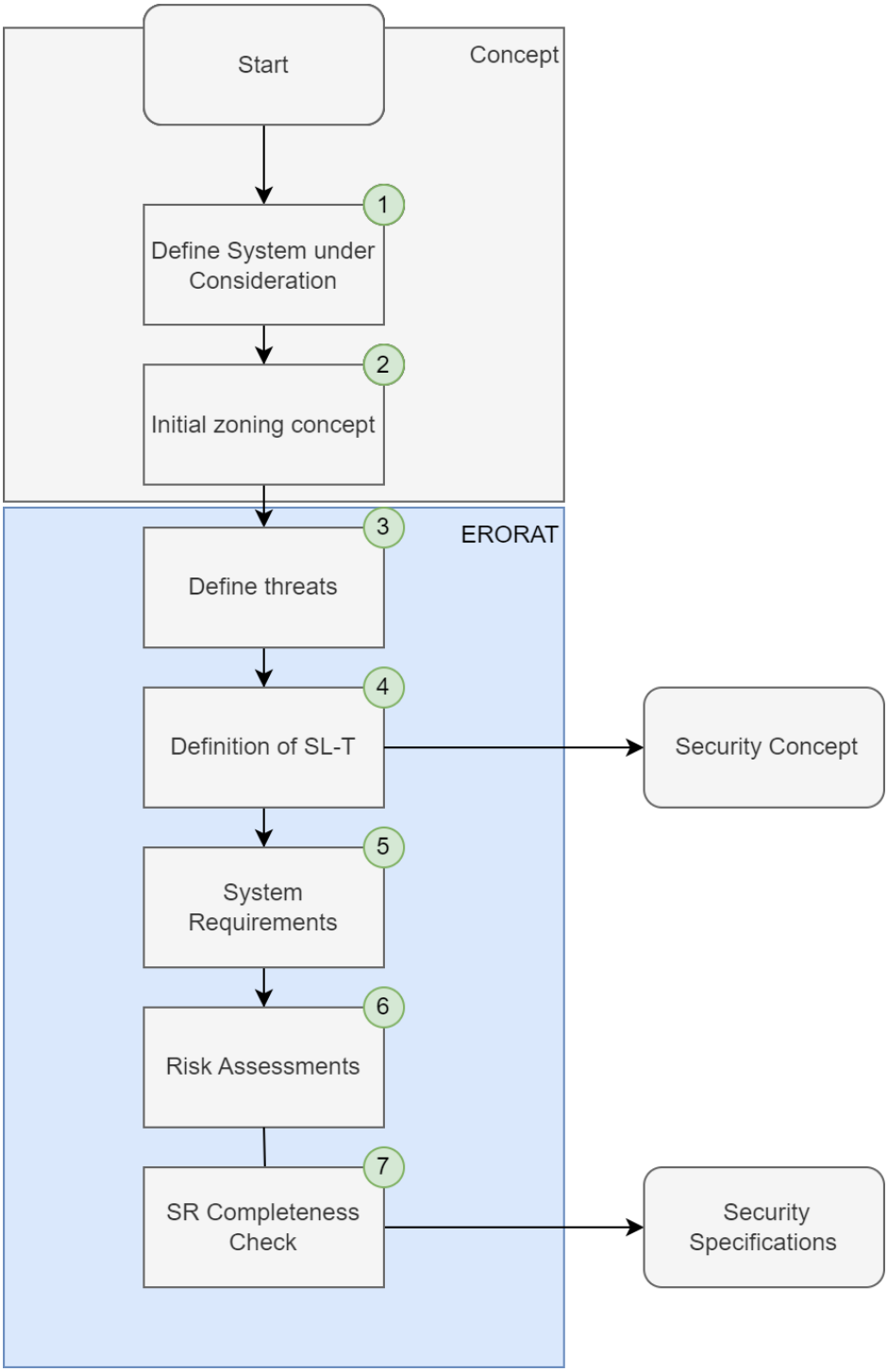

Figure 4: Security Process

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 [6])

3.2 Definition of Security Zoning

The System under Consideration (SuC) is the basis for defining security zones and conduits. Security zones defined in this process may not be equal to the physical and/or logical network zones of the SuC.

The aim of defining security 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 security zones can be analysed based on the protection requirements.

The security zone concept follows TS 50701 [6]. The integration and application of the security zone model is highly depending on the IM/RU system under consideration, also due to legacy systems or processes.

3.2.1 Rules used to define Security Zones and Conduits

The following rules are defined and applied:

Security Zones are groupings of components and systems

- with the same or similar impact estimations,
- with similar operational and functional characteristics,
- and at one location.
  (Note: the same zone definition can appear at multiple locations)

Conduits connect security zones

Remarks regarding differences between network and security zones:
Security zones are not equal to network zones (e.g., defined by VLANs).

Security zones are logical groupings of elements to allow efficient security analysis (risk and threat analysis), and are used to derive security requirements for the system.

Network zones implement network segmentation with security gateways, firewalls and VLANs. Network zones only partially implement security requirements of a security zone.

3.2.2 Usage of Security Zone and Conduits in ERORAT

To continue the process after step 4 of the security process (Figure 4) in the ERORAT tool the following steps should be implemented:

1. Use the ERORAT excel file and create one file per security zone.

   To avoid not manageable Excel-tables and unsecure Macros, it was decided to only assess one security zone per Excel file. So, for each security zone, a single Excel file shall be used.

2. Provide security zone name and additional descriptions, like assumption (if needed) to Tab “Zone definition”

3. Decide which connections (via conduit) are considered in the assessment of this security zone (Tab “Zone definition”)

   Conduits are not assessed in the risk assessment. If a conduit shall be assessed, it has to be transferred into one or more new security zones.

3.3 Threats Definition

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

3.3.1 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.

The existing catalogue is defined based on BSI elementary threats and additional threats based on the BSI IT-Grundschutz Compendium. This catalogue is excluding threats which are expected to be addressed by the RAMS domain (e.g. Water, Fire, Assaults). The transfer of responsibility to RAMS regarding these threats must be agreed and confirmed.

Tab “Threats_SL”, Section “**G-3a** (Threat Catalogue)”

3.3.2 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 [2]. This is to ensure conformity with TS 50701 [6] that refers to IEC 62443 [2] concerning the actual security measures. The mapping of threats to FRs is done based on three impact categories:

- Confidentiality (C)
- Integrity (I)
- Availability (A)

For each pair of threat and FR a combination of impact categories can be assigned. The assignment of an impact category is used if the corresponding FR can potentially mitigate the impact for the threat scenario.

Based on this mapping the SL-T is defined and relevant SRs (IEC 62243 [2]) are selected.

There are seven Foundational Requirements (FR) in place, the identified threats and corresponding impacts 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 “**G-3b** (FR)”

3.4 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 definition of the SL-T is defining the set of measures for the later phase of risk mitigation. It does not automatically require a SL-T x certification. The relevant, to be met requirements are the detailed requirements based on IEC 62443-3-3 and -4-2 in the according specifications resulting from this process.

The result is the final target Security Level for each security zone, SL-T.

Tab “SL-T”, Section “SL-Vector – **G-4e**”

The whole process is displayed in Figure 5, whilst the sub steps are explained beneath.

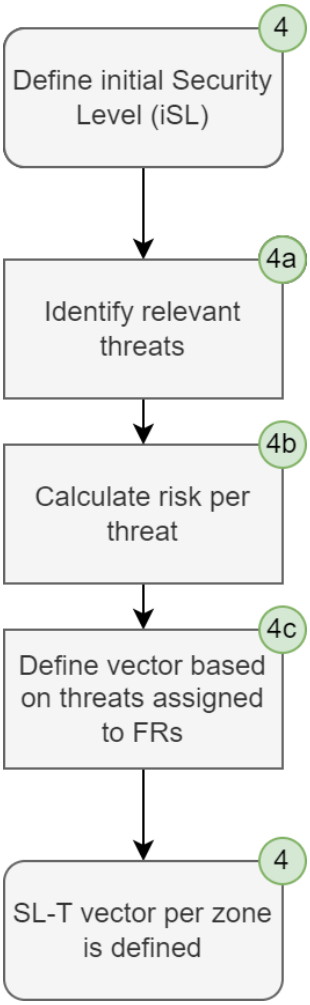

Figure 5: Define initial Security Level Subprocess

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

After the threats have been sorted to the FR in the process step number 4 (see Chapter 3.3.2), the relevant threats for the security zone must be identified.

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

Tab “Threats_SL”, Section “G-4a – Relevance”

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

Tab “Threats_SL”, Section “G-4b – Explanation / Reason why not relevant”

Hint: The RAMS requirements, like natural disasters, very often are not considered in the security assessment as there are analysed and managed by other project parts (Safety concept, Reliability concept, Maintenance concept). This can be noted and selected here.

- **5b: Calculate risk per threat**

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

The risk is defined similar to the calculations used in the risk assessment. Details can be found in Chapter 3.6.3. Impact and likelihood definition is done without taking any existing security measures or implementation of security features into account.

Values for exposure and vulnerability are used to calculate the risk similar to the risk assessment method.

Tab “Threats_SL”, Section “G-4c”

The impact is defined one per impact category, to allow for an assignment to the FRs based on the defined mapping:

- Confidentiality (C)
- Integrity (I)
- Availability (A)

The maximum impact values should match the impact calculated during the zoning process.

Tab “Threats_SL”, Section “G-4d”

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

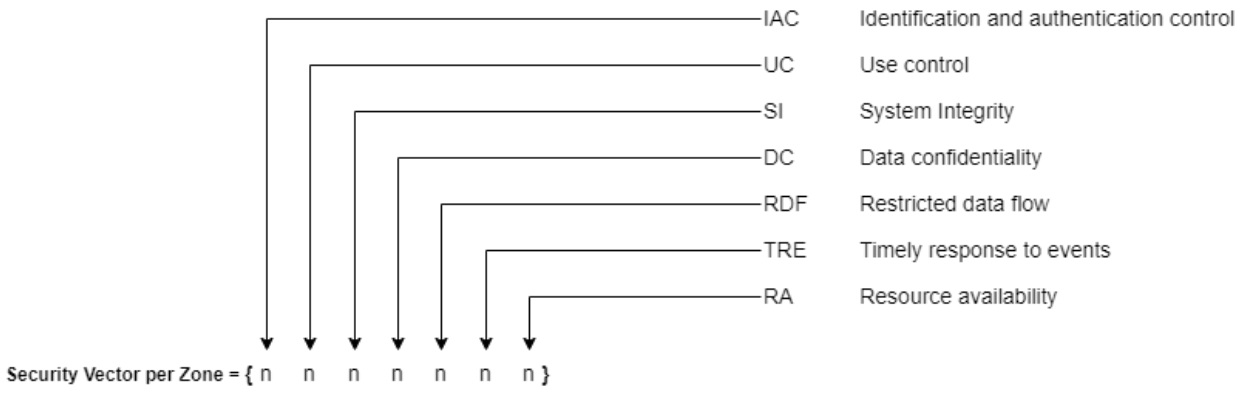

Figure 6: Security Vector

The SL-T vector (as defined in Figure 6) is calculated based on the following process:

The risk per impact category is calculated, e.g.:

Risk C = Likelihood + Impact C – 1

Threat	Likelihood	Impact C	Impact I	Impact A	Risk C	Risk I	Risk A
Threat 1	2	C	A	D	Significant	High	Medium

The risk per threat is transformed to an SL-T based on a predefined mapping: (Tab "SL")

SL-T C (Threat) = risk_to_SL(Risk C)

Threat	Risk C	Risk I	Risk A	SL-T C	SL-T I	SL-T A
Threat 1	Significant	High	Medium	**2**	3	**1**

Depending on the assignment of impact categories to FRs the highest SL-T is calculated for each FR per threat.

Threat	IAC	UC	SI	DC	RDF	TRE	RA
Threat 1	**CA**	**CA**	-	**C**	**CA**	**A**	**A**

Threat	IAC SL-T	UC SL-T	SI SL-T	DC SL-T	RDF SL-T	TRE SL-T	RA SL-T
Threat 1	max(**2**,**1**)	max(**2**,**1**)	max()	max(**2**)	max(**2**,**1**)	max(**1**)	max(**1**)

Threat	IAC SL-T	UC SL-T	SI SL-T	DC SL-T	RDF SL-T	TRE SL-T	RA SL-T
Threat 1	2	2	0	2	2	1	1

The maximum value of all threats per SL-T for an impact category is calculated.

SL-T(FR) = max (SL-T of all FRs)

Threat	IAC SL-T	UC SL-T	SI SL-T	DC SL-T	RDF SL-T	TRE SL-T	RA SL-T
Threat 1	2	2	0	**2**	2	1	**1**
Threat 2	2	2	0	**2**	2	0	0
Threat 3	**3**	**3**	**3**	1	**3**	**3**	**1**
Max	3	3	3	2	3	3	1

A resulting vector could look like this:

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

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

SL-T = max (SL-T vector)

In this example the SL-T value is:

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

Tab “SL-T”, Section “SL-Vector – G-4e”

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

3.5 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 “Measures_62443-3-3”. The update filter function must be used to see the relevant SRs after a change in the SL definition.

3.6 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 security zone.

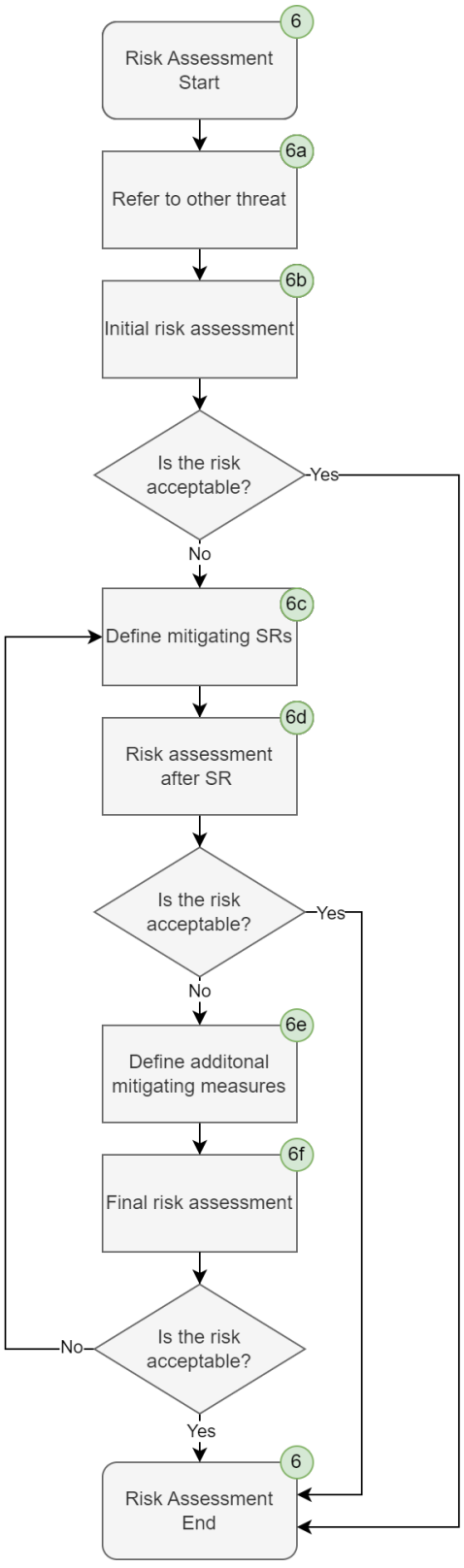

Figure 7: Risk Assessment

By applying this process, the following goals are achieved:

1. Fully performed security evaluation process following TS 50701 [6]
2. Measures applied following IEC 62443 [2]
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.

3.6.1 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 – G-6”

3.6.2 Risk Assessment Process

The following steps are used to perform the risk assessment (as shown in Figure 7):

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 “G-7a”

b) Unmitigated risk assessment

The unmitigated risk assessment is carried out without considering any new measures. For legacy systems prefulfilled measures are taken into account. Thus, it is based on the systems current architecture.

The risk is evaluated according to Chapter 3.6.3.

Exposure, Vulnerability and Impact is automatically transferred from Tab “Threats_SL”. These values have been assigned according to Chapter 3.4 without taking any existing security measures or features into account. If e.g. a legacy system is assessed, existing security measures can be taken into account already in the initial risk assessment step. This can result in lower resulting values for exposure, vulnerability and impact compared to Tab “Threats_SL”. These lower values can be entered in the corresponding sections marked with “Override” and will automatically be included in the risk calculation. Pre-fulfilled SRs can be selected in Tab “Measures_62443-3-3” using the marking “P”. Furthermore, additional measures can be described.

If the risk is accepted according to Chapter 3.6.4 the process for this threat is finished.

Tab “Risk_evaluation”, Section “G-7b”

c) Define mitigating SRs

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

Tab “Risk_evaluation”, Section “G-7c”

The selection of SRs is performed in Tab “Measures_62443-3-3” using the “M” marking.

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 3.6.3.

If the risk is accepted according to Chapter 3.6.4 the process for this threat is finished.

Tab “Risk_evaluation”, Section “G-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 “G-7e”

If IEC 62443-2-1 measures are used the selection is performed in Tab “Measures_62443-2-1”.

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 3.6.3.

If the risk is not accepted according to Chapter 3.6.4 the process needs to be continued at c).

Tab “Risk_evaluation”, Section “G-7f”

3.6.3 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 [2] 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 [6] (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 [6] (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 [6] (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 [6]. 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”

3.6.4 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.

  Tab “Risk_evaluation”, Section “G-7e”

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

3.7 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 security zone (e.g., SR for radio connections if not radio connection exists) – Mark corresponding SR in Tab “Measures_62443-3-3” with “Relevance revoked” = “Yes”

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.

Tab “Measures_62443-3-3”.

3.7.1 SL Consistency Check

To provide a better overview of the SL which can be achieved using the selected SRs, ERORAT provides Tab “SL-T”, Section “G-8a”. This view provides a consistency check and indicates if the defined SL-T can be achieved using the selected SRs either initially (pre-fulfilled) or after additional mitigating SRs are applied.

Revoked SRs are ignored in the calculation of the SL check values. E.g. by marking a SL 4 SR which is not applicable as revoked, SL 4 can still be achieved.

3.7.2 Maximum SR Selection Check

An SL is defined for each FR starting from which it must be implemented. This value is used to generate Tab “SL-T”, Section “G-8b” which shows the maximum SL associated with a selected SR. If e.g. one SR 1.7 RE 2 is selected, which is required starting with SL 4, the corresponding maximum value for IAC will be 4 independently if other SL 4 requirements (or lower) are selected. If for example SL-T for IAC equals 3, but multiple SL 4 System Requirements have been selected in the risk assessment to mitigate remaining risks, the automatically selected SL might not be correct. In this case, the security expert could decide to increase the SL value. Only the views simplifying this check are implemented in ERORAT. If the SL is adjusted, this has to be performed in the corresponding documentation (e.g. Security Concept).