RCA

Reference CCS Architecture

An initiative facilitated by the ERTMS Users Group and the EULYNX consortium

OCORA

Open CCS On-board Reference Architecture

(Cyber) Security Guideline

Document id: RCA.Doc.45

Revision history

Version	Change Description	Name (Initials)	Date of change
0.01	Initial draft	Ulrich Meier Roger Metz Max Schubert	2020-10-22
0.02	Security Cluster 1st review integration	Ulrich Meier Roger Metz Max Schubert	2020-11-04
1.0 (0.A)	Approval by RCA CG for BL1 R0	Mirko Blazic	2021-02-04

Table of Contents

Table of Tables

Table of Figures

1 Introduction

1.1 Release information

Basic document information:

RCA.Doc.45

(Cyber) Security Guideline

Cenelec Phase: n/a

Version: 1.0 (0.A)

RCA Baseline set: 0

Approval date: 04.02.2021

1.2 Imprint

Publisher:

RCA (an initiative of the ERTMS Users Group and EULYNX Consortium)

Support and Feedback

For feedback, or if you have trouble accessing the material, please contact rca@eulynx.eu.

1.3 Terms and Abbreviations

The terms and abbreviations are listed in the EULYNX and OCORA Glossary.

1.4 Purpose of the document

This document is published as part of the OCORA Gamma release and in EULYNX and RCA in the context of the Security Cluster publications for baseline 4. It is the first release of this document and it is in a preliminary state.

Subsequent releases of this document and topic specific documentation will be developed in a modular and iterative approach, evolving within the progress of the RCA, EULYNX and OCORA collaborations.

This document aims to provide the reader with:

- A guideline to and definition of a harmonized Security Risk Assessment for System Design process

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 RCA, EULYNX and OCORA.

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

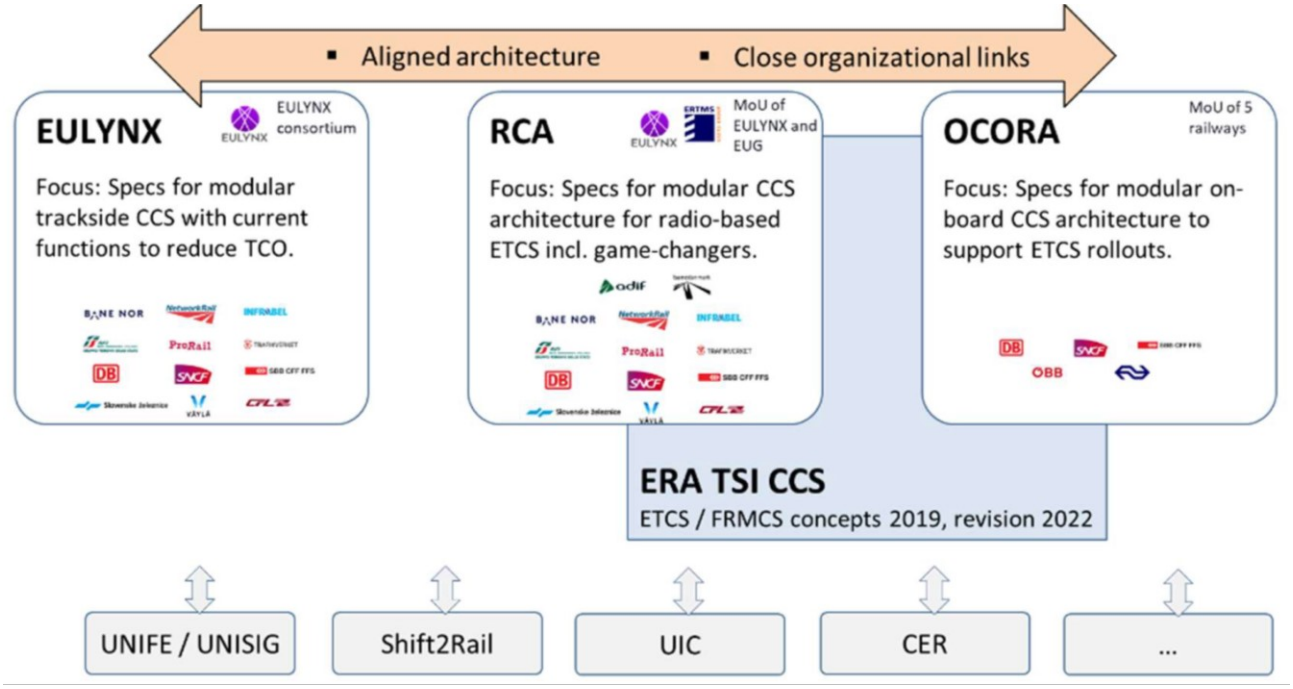

Figure 1 Relations of EULYNX, RCA and OCORA[1]

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

The reader will be able to provide feedback to the authors and can, therefore, engage in shaping the security approach.

1.5 References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references.

The following references are used in this document:

[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] EULYNX Baseline 3 Release 5

[5] IEC 62443 3-3 - Industrial communication networks – Network and system security –Part 3-3: System security requirements and security levels

[6] ISO 27005

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

[1] Source: https://eulynx.eu/index.php/news/61-rca-gamma-published, Concept: Architectural approach and System-of-system Perspective. TCO: Total Cost of Ownership

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

[9] OCORA 40-008-Gamma – Security Overview

[10] OCORA-10-001-Gamma – Release Notes

[11] OCORA-20-001-Gamma – Program Slide Deck

[12] OCORA-20-002-Gamma – Technical Slide Deck

[13] OCORA-20-004-Gamma – Technical Posters

[14] OCORA-30-001-Gamma – Introduction to OCORA

[15] OCORA-40-001-Gamma – System Architecture

[16] OCORA-90-002-Gamma – Glossary

[17] prTS 50701 - Railway Application – Cybersecurity (Version D8E5)

[18] RCA Baseline 0 Release 1

[19] VDE V 0831-104: 2015-10

Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). We always reference to the latest available official version of the SUBSET, unless indicated differently.

2 Management Summary

One of the main objectives of the RCA/EULYNX 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 RCA, EULYNX and OCORA.

This is joint venture document from the EULYNX/RCA and OCORA security workgroups.

EULYNX/RCA:

Max Schubert (DB, external), Ulrich Meier (SBB, external)

OCORA:

Roger Metz (SBB, external)

3 Guideline Definitions

3.1 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, to apply the security engineering processes proven in other industries, e.g. IEC 62443 [5]. The upcoming standard EN 50701, currently as prTS 50701[17], expected mid-2021, 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. 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 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.)

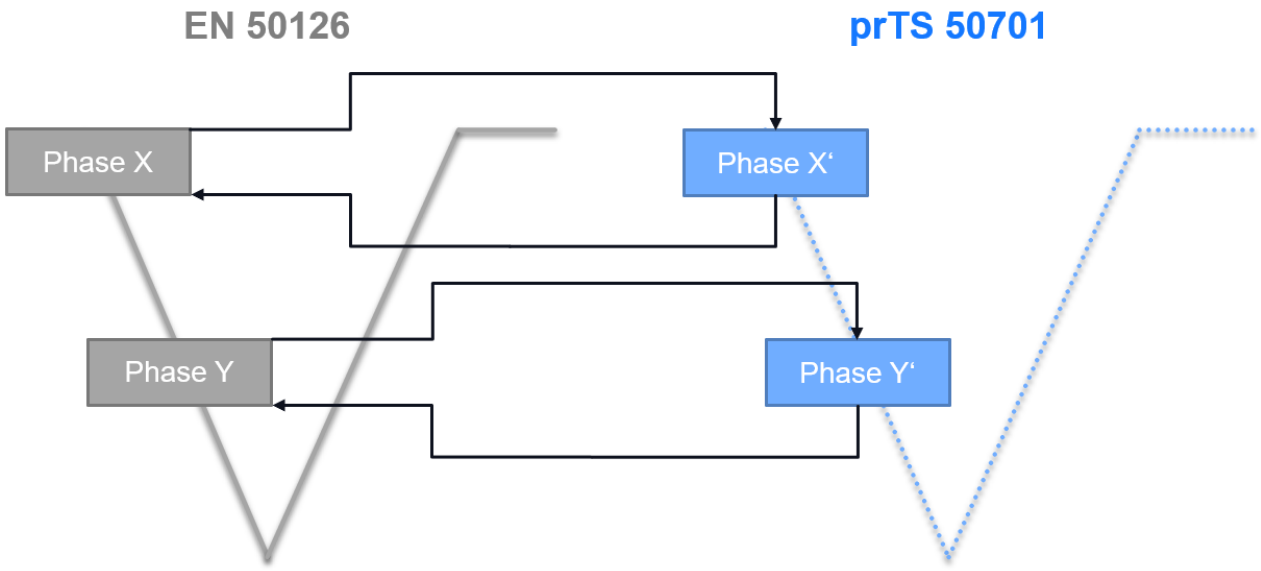

Figure 2 Process Interaction

Security solutions are not subject to assessment in contrast to railway solutions, which are developed according to EN 50126. 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 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 prTS 50701. The result of each stage 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 stages 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 and prTS 50701. 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. A more detailed example is presented in the appendix (chapter 6.2).

	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	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 Zones and Conduits	Threat context Initial Threat Log Potential updates (like zones or network plans)	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

3.2 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 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[6]:

The ISO-standard is focussing on security risk management for organisations in the context of the ISO 27000 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[7]:

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 [5]:

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.

prTS 50701 [17]:

This technology standard and technical speficiation are mainly based on IEC 62443 and references also NIST 800-30**Error! Reference source not found.**. 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 [19]:

This German (pre-) standard is referenced and based on IEC 62443, as it was developed similarly to the prTS 50701**Error! Reference source not found.** and it ads 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.

3.3 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 Zone Concept

2 Threat Analysis

3 Risk Analysis (structural analysis)

4 Measures

5 Integration / Security Architecture / Specification

3.4 Security Risk Assessment Approach

There are two approaches to define the security measures based on a risk analysis. Following the standards, NIST **Error! Reference source not found.Error! Reference source not found.**, IEC 62443 **Error! Reference source not found.**, ISO 27005 **Error! Reference source not found.** 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 - audit capability - proven measure - easy to commonly agree on - can be set into relation of process from EN 50126 **Error! Reference source not found.** / Safety approach	- taking the actual function of the system into relation - 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 - may be more “expensive” than the functional approach	- no back-up by a standard - risk of forgetting attack methods (forget to secure the hidden champion) - not one by one connectable to safety (EN 50126 **Error! Reference source not found.**) - 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.

4 Process Definition

In this chapter the whole process for the risk assessment is described, which is based on the decision of chapter 3.2 to use prTS 50701 as the basic standard.

The definition starts in chapter 3.3 and 3.4 with an evaluation on the risk assessment approach chosen for the RCA, EULYNX and OCORA clusters to ensure a common risk evaluation process.

In chapter 4 the process is defined, the process itself is presented with all steps and each step is described in the following chapters, starting with chapter 4.1.

For having an example for each step chapter 5 provides a full walk through for trackside CCS[1] (EULYNX, RCA; an example for onboard CCS (OCORA) will follow in the next revision).

Further, the process is applied to all EULYNX, RCA and OCORA architecture elements in ERORAT "EULYNX_RCA_OCORA_Risk_Assessment_Calculation.xlsm" in the Appendix Ch. 6.1. This Excel file is meant to be the risk assessment tool for EULYNX, RCA and OCORA and with this named – ERORAT (EULYNX RCA OCORA Risk Assessment Tool).

ERORAT allows to understand the process and use the model solution for the country specific IM implementation to respect individual needs and legacy systems. Only as mandatory declared requirements from EULYNX/RCA/OCORA-perspective need to be followed to ensure compatibility to the standard interface specifications.

ERORAT leads you 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 was defined, based on IEC 62443 and prTS 50701:

1. Define system under consideration (SUC) (prTS 50701, IEC 62443) following the RCA, EULYNX and OCORA Architecture
2. Initial zoning concept based on initial risk assessment
3. Define attacker types (generic)
4. Evaluation of the attackers, strength, motivation, 3 Factors (generic) according to IEC 62443
5. Threats e.g. from the BSI catalogue, supplemented
6. Sorting of threats into the Foundational Requirements
7. Definition of the initial SL-T (iSL-T) per threat in FR. The max iSL in FR is the iSL of the FR.
8. The FR value is entered into the vector of the preliminary zone
9. After the max value of the vector for the zone is defined, the iSL for the preliminary zone is derived.
10. Reduction factors can now be applied (max 1) to determine the final SL
11. Now the measures according to IEC 62443 are applied
12. Check whether measure can be applied to preliminary zone concept while meeting the requirements. If not, zone concept needs to be revised.
13. Redo steps 11 and 12 until the final set up is found

In the following the process is inserted intoa flow chart in order to visualize it.

The whole process can be documented using ERORAT, where a model solution is displayed already.

[1] CCS: Command, Control, Signalling

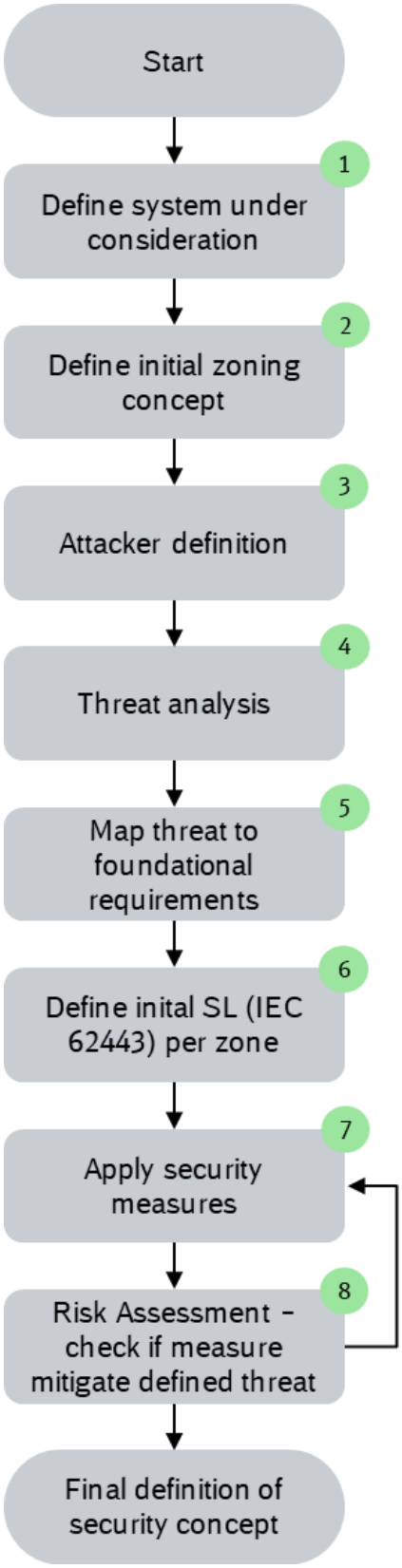

Figure 4 RCA/EULYNX/OCORA Security Process

All these steps are described in detailed in the following chapters (4.1 - 4.8).

A RACI matrix (responsibility, accountability, consulted, informed) can be applied to manage this process successfully. The project specific RACI matrix should be defined and available in a at least preliminary version when starting the process.

4.1 Define System under Consideration

The system under consideration is the RCA, EULYNX and OCORA architecture. The RCA architecture [18] is shown on high level as an example in the following picture:

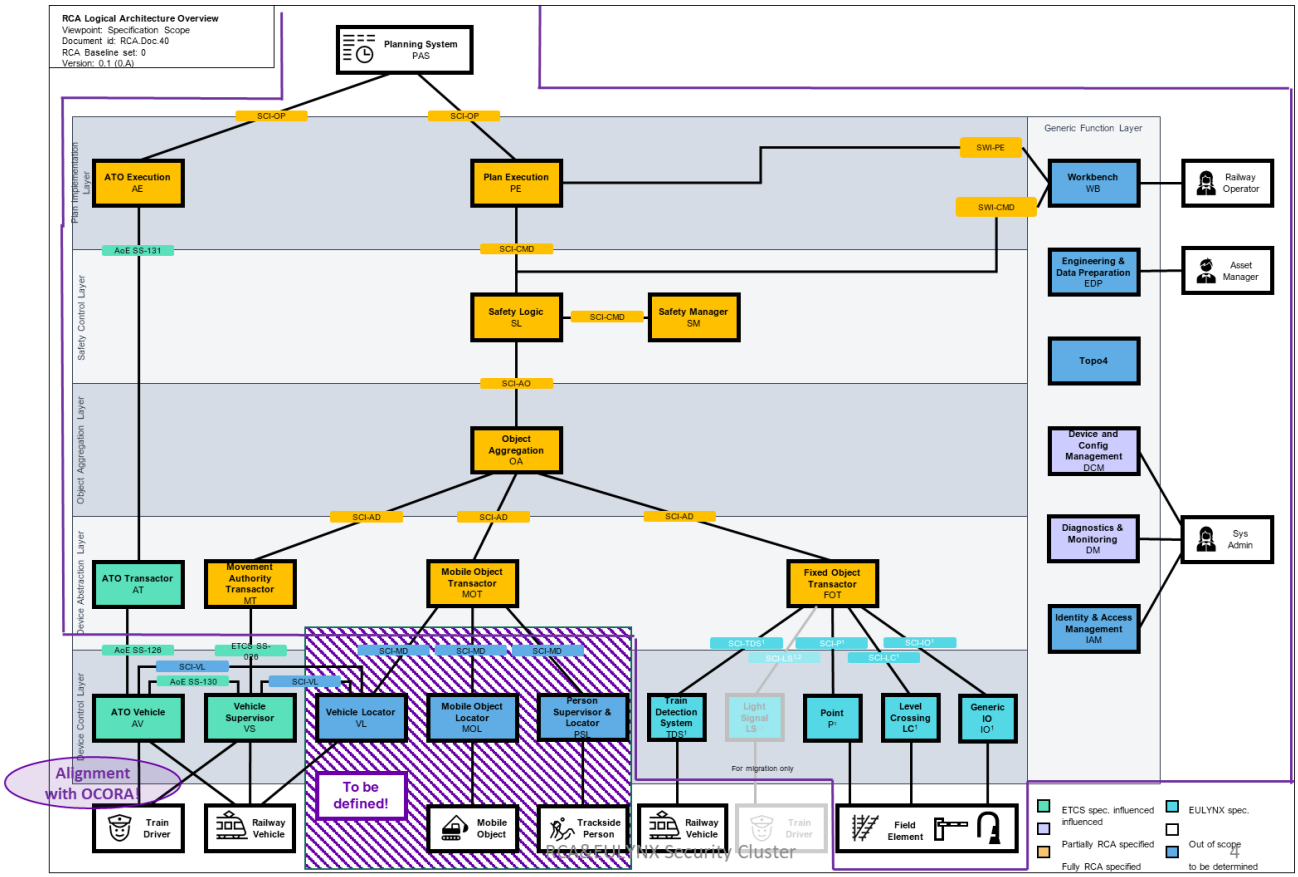

Figure 5 RCA

4.2 Definition of Zoning for Architecture

The system definition or system under consideration from chapter 4.1 is the basis for defining zones and conduits.

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 Risk Assessment is needed. This risk assessment is not part of ERORAT, since the definition of the zones and conduits for EULYNX/RCA/OCORA was fixed in the security clusters group and is not under further consideration with the infrastructure manager specific implementation. In principle the same process as in the risk assessment for the zones and conduits, performed in chapter 5.8, was gone through for every component or partial system to group the zones and conduits.

The architectural designs are given from RCA, EULYNX or OCORA. The zone concept follows prTS 50701. The integration and application of the zone model in each country is dependent of IM or vehicle specific situation due to local legacy systems or processes.

4.3 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 definition of the term attacker is used. The attacker does not have to be a person, even if the term suggests it. Attacking here means

"to cause damage". In this interpretation, lightning is also an attacker because of its damaging effect. The determination of the severity of a threat event follows the system of the IEC 62443**Error! Reference source not found.**, referenced in prTS 50701, after which the type of attacker and its possibilities are defined.

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

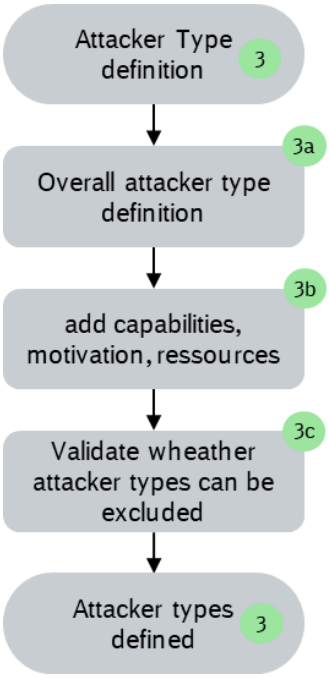

Figure 6 Attacker Definition

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

The attacker definition is the basis to allow classification of the threats and to define a likelihood. Attacker types can be divided into five categories:

1. Intentional, targeted attacker

   These are persons who intentionally damage the IT of the CCS-System. Targeted attackers are the focus of the analysis. To this category is also the orientation of the standard IEC 62443. Evaluation methodology that evaluates, among other things, attacker motivation and skills.

2. Human failure, untargeted actions

   The CCS system gets attacked unintentionally in this category and randomly through mistakes such as operating errors or negligent actions. The system is more likely to be damaged by accident, mostly by authorized persons.

3. Technical failure

   In the event of a technical failure, the cause comes from the system itself in the form of malfunctions, malfunctions, and failures. On the one hand, this category is the focus of functional safety and is controlled there with appropriate measures, on the other hand, the availability within the IT security management is intensively so that this type of attacker is only considered in a limited way.

4. Environmental influences and force majeure (environment)

   In this case, harmful environmental factors such as low or high temperature or the beforementioned lightning to the CCS system. This category is not considered further since the resulting threats are controlled by the very basic security measures.

   Comment: Environmental influences are not further elaborated within this Excel file (EULYNX_RCA_OCORA_Risk_Assessment_Calculation) since it is a very local definition. Any way it is highly recommended to take those into account to ensure availability of the overall railway system.

5. Organizational

   Organizational failure is often found to be another type of attacker. This includes including insufficient, incorrect, or unclear processes, specifications, or responsibilities. This attacker type was not included

here, since these organizational weaknesses do not attack the CCS system directly, but upstream of the threat events are. They only come into play again when safety measures are established.

- **3b: Add Capabilities, Motivation, and Resources**

In the next step the capabilities, motivation and resources are added to each attacker type. This step is later used to elaborate the likelihood of a successful attack and its impact which directly leads to the needs security level (SL). For this purpose, the following table from IEC 62443 **Error! Reference source not found.** is used.

		Resources		
		2 Low	3 Moderate	4 Extended
Know-ledge	2 General	iSL 2	iSL 3	iSL 4
	3 Specific	iSL 3	iSL 3	iSL 4
	4 Extended	iSL 3	iSL 4	iSL 4

Table 3 Attacker Knowledge and Resources

Tab “attacker_threats_zones”, column “attacker”, “3b”

The result of the combination of the attacker and its resources and knowledge leads to a SL-value which will be used in combination with each of the threats.

Tab “attacker_threats_zones”, column “SL”, “iSL- 3b”

- **3c: Attacker Types Exclusion**

Theoretically every possible attacker type, environmental effect and catastrophe can happen. One could imagine an asteroid shower falls on your railway network or every other country in the world has interest to harm your system. This would lead to massive security requirements that cannot be met and maintained or financed. Therefore, in the third step of defining attackers, it is possible to exclude attacker types. This should be based on a current elaboration of the threat situation. For this purpose, threat analysis from governmental organization can be considered. Some examples are presented here:

Austria:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AT_NCSS.pdf

https://www.bundeskanzleramt.gv.at/en/topics/security-policy/cyber-security.html

France:

https://www.interieur.gouv.fr/content/download/117535/942891/file/Rapport-Cybermenaces2019-HD-web-modifi%C3%A9.pdf

Germany:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf?__blob=publicationFile&v=7

Great Britain:

https://rusi.org/sites/default/files/201406_bp_the_threat_of_cyber-crime_to_the_uk.pdf

Switzerland:

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf

As the reason for excluding some attacker types may change over time or due to a change in the threat landscape, It is wise 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.

4.4 Threat Analysis

The CCS system is not a completely new technical and organizational system within Railways. CCS has existed for a very long time and has therefore already implemented security in many ways. It is also subject to the corporate and group-wide guidelines for the use of IT. For these reasons, assumptions are made, i.e.

certain protective measures and threats in this regard are not followed up. On each assumption the basis on which it was taken shall be recorded. Overall threat landscapes are available on UIC, CERT-EU, ENISA, national intelligence etc. Theses assessments influence the relevance of attacker types and risk assessments for each country.

Tab “attacker_threats_zones”, column “threats”, “threat catalogue - 4”
Several threats are already controlled within the IM specific environment due to its “history”. The general assumptions for electrical railroad signalling systems therefore apply. The assumptions made are named AS.type, as AS stands for assumption. This follows in principle naming convention introduced in the prTS 50701.

AS.Access

It is assumed that all technical, organizational and personnel measures for the protection of the infrastructure manager’s property/equipment are implemented in accordance with the IM/operator specific rules.

This is in order to ensure the security of customers, employees, tangible and intangible assets and business processes against physical attacks.

Such physical attacks include burglary, theft, robbery, sabotage, espionage, bodily injury, vandalism and other criminal acts.

As a result, the physical security in general is not treated any further within this document.

This assumption does not apply to physical IT components positioned in the track field. This concerns components in the field element junction box and in track field concentrators.

AS.Environment

As earlier discussed, environment is IM/operator specific. That is why, it is assumed that there is sufficient protection against environmental threats and force majeure, which is a general safety task that affects all areas of railroad operations. An example related to EULYNX would be the protection of the outdoor cabinet by tree pruning or protective measures against rockfall.

AS.Operator

It is assumed that operator’s personnel are sufficiently trained for the tasks assigned to them to apply the IT security functions they use correctly and in accordance with the IT security policy. It is assumed that the operators are trustworthy within the scope of the tasks assigned to them and do not carry out intentional attacks (exclusion of internal offenders)[1]. In the CCS environment, the operators must have the necessary authorizations to perform their tasks. This requires appropriate technical training. According to this it is assumed that operation of the control and command systems is not permitted without such training and further necessary and recommended measures. Further, it is assumed that the infrastructure manager or operator has a “real-time” knowledge of who is authorised for each relevant location.

AS.SecPol

It is assumed that the personnel and organizational requirements of the IT security policy are met with the help of an existing ISMS. This is usually required by the framework of the CIO or CISO. This also includes the protection of system components against tampering and manipulation, which are necessary for the implementation of the IT security policy.

AS.Installation

It is assumed that IT security in the procurement and installation of technical systems is considered and guaranteed.

AS.Maintenance

It is assumed that there is sufficient protection against disturbances and malfunctions of hardware or software components. This is the core task of functional safety.

[1] Every IM or vehicle operator must assess if the assumption “no internal offender” is valid for his current and expected situation and the respective system under consideration and usage scenario.

4.5 Threat Mapping to the foundational Requirements

In this step the identified threats are mapped to the foundational requirements (FR) from IEC 62443. This is to ensure conformity with prTS 50701 that refers to IEC 62443 concerning the actual measures. So, this step is the preparation to choose the right measures in dependency of the needed security level according to IEC 62243, later.

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 requirement area threats are classified, 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 requirement area threats are classified, which lead to an unauthorized use of the system.
3. System integrity (SI - System integrity)
   In this requirement area, threats are classified that are manipulable of data or components.
4. Confidentiality (DC - Data confidentiality)
   In this requirement area, threats are classified that lead to unauthorized lead to knowledge or disclosure of data or information.
5. Restricted data flow (RDF - Restricted data flow)
   In this requirement area, threats are classified that lead to inadmissible manage 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 classified in this requirement area.
7. Availability of resources (RA - Resource availability)
   Threats that interrupt your resource flow that guarantees smooth operation, e.g. energy supply.

This process can be followed in the EULYNX_RCA_OCORA_Risk_Assessment_Calculation.xlsm again.

Tab “attacker_threats_zones”, column “threats”, “FR - 5”

4.6 Define initial Security Level per Zone

The definition of the initial target SL (iSL) is necessary to have a documented basis for choosing the fitting measures to ensure security for the system. For this purpose, a formal process is applied. Here, again, the EULYNX_RCA_OCORA_Risk_Assessment_Calculation.xlsm helps with following this procedure.

The result is the final target Security Level for each zone, SL-T. Tab “iSL-SL-T_zone”, row “SL-T – 6”

The whole process is displayed here, whilst the sub steps are explained beneath the following Figure 7.

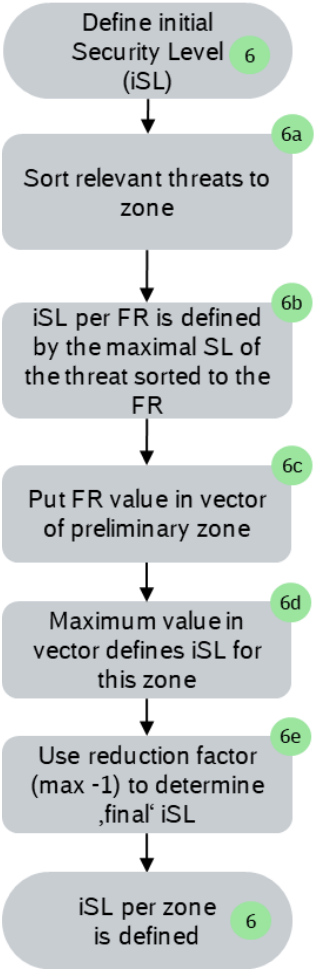

Figure 7 Define initial Security Level Subprocess

- **6a: Sort relevant Threats to Zones**

After the threats have been sorted to the foundational requirements in the step number 5, they are now sorted to zones and conduits. Each threat can be relevant for multiple zones and conduits so for each threat it is a 1:n relation. In chapter 5.6 the process is shown with an example.

The EULYNX_RCA_OCORA_Risk_Assessment_Calculation.xlsm uses a matrix to mark which threat is relevant for which conduit and zone, so that there is a quiet clearly arranged view available.

Tab “attacker_threats_zones”, column “zone/conduit relevance – 6a”

- **6b: Definition of iSL per FR by the maximal SLs of the threats sorted to the FR**

For the next step, the initial Security level (SL) per foundational requirement (FR) is defined. The SL is defined by the threat with the highest request. So, there is no average or weighing made but the maximum possible threats marks the need.

Tab “iSL-SL-T_zone”, column “zone/conduit – 6b”

- **6c: Put FR Value in Vector of preliminary Zone**

After the definition per FR, all FR per zone are taken together in the zone vector. So, each zone has 7 FR SL values. A vector looks like this: iSL = {1,2,3,3,2,1,3}

Tab “iSL-SL-T_zone”, row “Vector – 6c”

- **6d: Maximum Value in Vector defines**

Now the initial SL for each zone and conduit needs to be calculated. Here, again, the maximum SL in the vector marks now the initial SL for the whole zone. With this step one has the initial SL set for the zone or conduit. So, in the above example the zones iSL would be 3. iSL = {1,2,**3**,**3**,2,1,**3**} = **3**

Tab “iSL-SL-T_zone”, row “iSL – 6d”

- **6e: Use reduction Factor to determine target SL**

In the last step reduction factors can be put in place. These factors follow norm VDE 0831-104 and especially related to railway needs. The maximum reduction of the needed SL-level is 1.

Tab “iSL-SL-T_zone”, row “reducing factor – 6 e”

4.7 Apply Security Measures

In the following the security measures are chosen and applied. Therefore, it is important to understand that the measures should avoid security risks in the first step. IEC 62443-3-3 chapter 5-11 displays the standard measures to reach that goal. Since each IMs installation is specific, it might be that some measures are not ideal or not even possible to implement. This evaluation should be done very carefully since it has massive impact on costs for investment and operation. That is why in the further process it is evaluated whether the measure can be applied, and the explanation is added. After this step compensating measures or risk acceptance shall be taken into consideration.

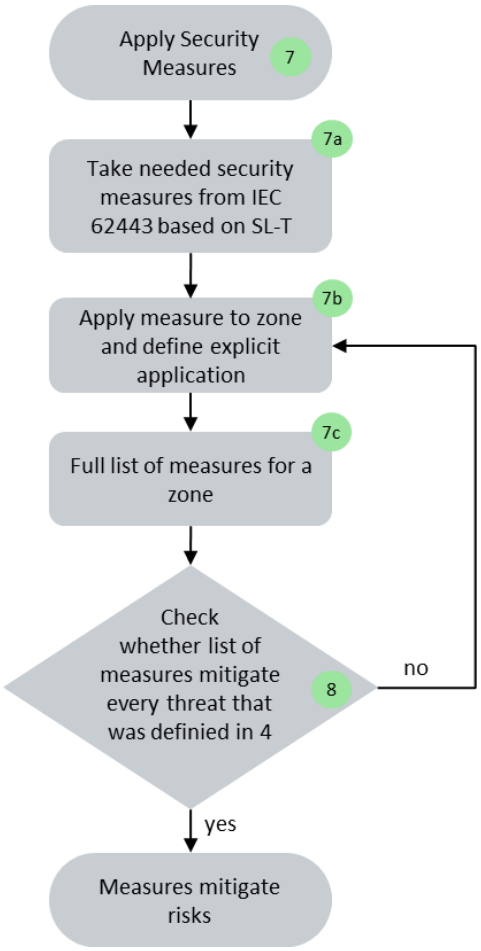

Figure 8 Apply Security Measures Subprocess

- **7a: Map Security Measures according to IEC 62443 based on SL-T**

In this step the measures according to IEC 62443 are chosen for the earlier defined SL-T level per zone. These measures are now a requirement to be fulfilled by the system, component, or process to ensure the calculated security level of the zone or conduit.

Tab “Measures_interlocking ”, column “Measure – 7a”

- **7b: Apply Measure to Zone and define explicit Application**

In the next steps it needs to be documented how the measure is applied. That means the requirement from the norm is translated into an applicable requirement which takes the actual system design in consideration.

Tab “Measures_interlocking ”, column “Application in …. – 7b”

- **7c: Full list of applicable measures**

After steps 7a and 7b one has a list of all applicable measures. In the result it will turn out that not every measure was applied as the norm it requires. That is why the next step is needed.

4.8 Risk Assessment

Step 8 displays the actual risk assessment. Here it is checked whether the measures could mitigate the risks and the target risk level – usually low – could be reached.

For this purpose, the following steps need to be performed:

- **Definition of the target risk** Tab “Risk_evaluation_... “, column target risk – 8.1”

  Default target risk = Low

- **Evaluation of the actual risk by using the following steps and calculations**

  The risk is evaluated before measures have been applied, after IEC 62443 measures have been applied and after additional compensating measures have been applied. Thus the risk has to be evaluated in three steps. If no measures are applied after a risk evaluation the risk does not have to be reevaluated.

  a) Evaluation of the exposure of the system

  This is performed by using the standardised exposure categories from 1 to 3, based on prTS 50701 (Tab “Risk calc basis”). The result of this evaluation, which is usually performed with a group of experts, is documented. Tab “Risk_evaluation_... “, column Exposure – 8.2a”

  b) Evaluation of the Vulnerability of the system

  This is performed by using the standardised vulnerability categories from 1 to 3, based on prTS 50701 (Tab “Risk calc basis”). The result of this evaluation, which is usually performed with a group of experts, is documented. Tab “Risk_evaluation_... “, column Vulnerability – 8.2b

  c) Evaluation of the Impact of a fail or manipulation of the system

  This is performed by using the standardised impact categories from A to D, based on prTS 50701 (Tab “Risk calc basis”). The result of this evaluation, which is usually performed with a group of experts, is documented. Tab “Risk_evaluation_... “, column Impact – 8.2c”

  The result of 8.2a and 8.2b is calculated to a likelihood in the categories 1-5 following prTS 50701. Tab “Risk_evaluation_... “, column Likelihood – 8.2ab”

  In the end the combination of likelihood and threats causes a risk.

  Tab “Risk_evaluation_... “, column Actual Risk – 8.2”

- **Evaluate risk delta**

  Now one steps into the evaluation if the measures have been successful to reduce the risk to the target level 8.1). If yes, the process is finished. The risk delta is now “0” and there is “nor risk acceptance needed”. Tab “Risk_evaluation_... “, column “risk acceptance delta” and “risk acceptance explanation”

  If this is not the case, compensating measures need to be performed

  Tab “Risk_evaluation_... “, risk delta – 8.3”

- **Compensation Measures**

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

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

  Tab “Risk_evaluation_... “, column “compensation measure – 8.4”

- **Final Risk Assessment**

After the possible and useful measures have been defined the final risk assessment is performed, following the steps from 8.2.

Tab “Risk_evaluation_... “, column “Final Risk Assessment – 8.5”

- **Final Risk and Risk acceptance**

  In the case there is a final risk that is higher than the target risk, so the delta is > 0, risk acceptance is the last possible solution. Risk acceptance then needs to be documented very clearly including why the risk can be accepted using comparison or a quantitative or qualitive value to demonstrate the possibility to accept.

  Tab “Risk_evaluation_... “, column “final risk 8.6” “risk acceptance delta” and “risk acceptance explanation”

This is the end of the Risk Assessment.

With finishing the process, one has achieved the following goals:

1. Fully performed security evaluation process following prTS 50701
2. Measures applied following IEC 62443
3. Definition of risk delta and risk acceptance, if needed
4. System requirement for Security

The process needs to be performed for every zone and conduit and within those for every threat.

5 Guideline Example Walkthrough

In the following the process is went through initially for EULYNX with the concentration on MDM, leading to measures for the Security Operations Centre. An example for vehicle solutions will be available in the next revision of this document.

5.1 System under Consideration

In the first step the system under consideration needs to be defined. For the walkthrough, the complexity is reduced to the EULYNX architecture [4] since this is defined in more detail already and so a zone concept can be applied in the next step. For this the logic EULYNX architecture is displayed first:

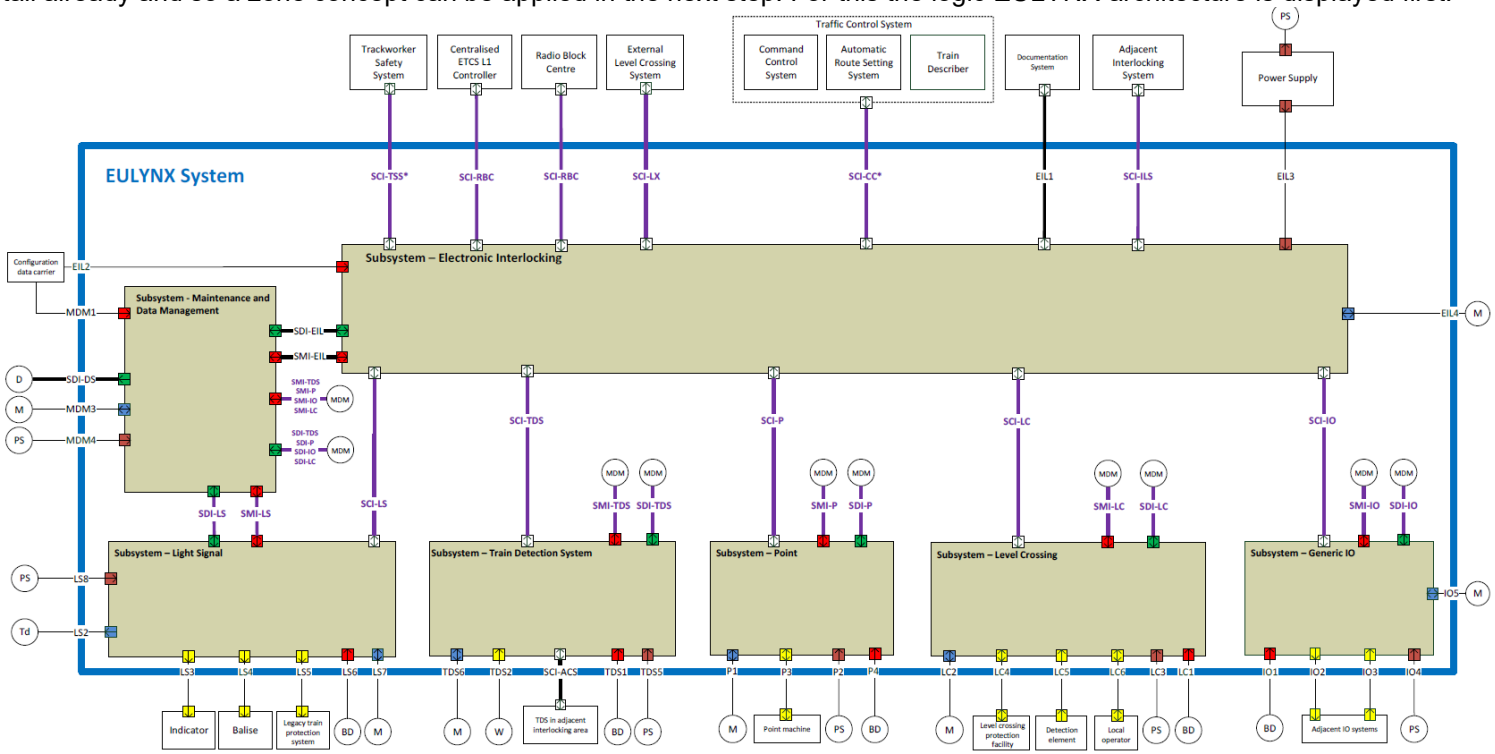

Figure 9 EULYNX Logic Architecture

The logic architecture does not allow to apply security zones, since it cannot be seen how the systems are sorted to an implemented architecture. This for one need to define a system definition that allows a location-based design, including housing and network concept. There for an assumption of a possible implementation is displayed as follows. Here only the relevant systems and their zones are displayed. Explicit system configuration and conduits are not foreseen in this example, but would need to be implemented for a complete picture:

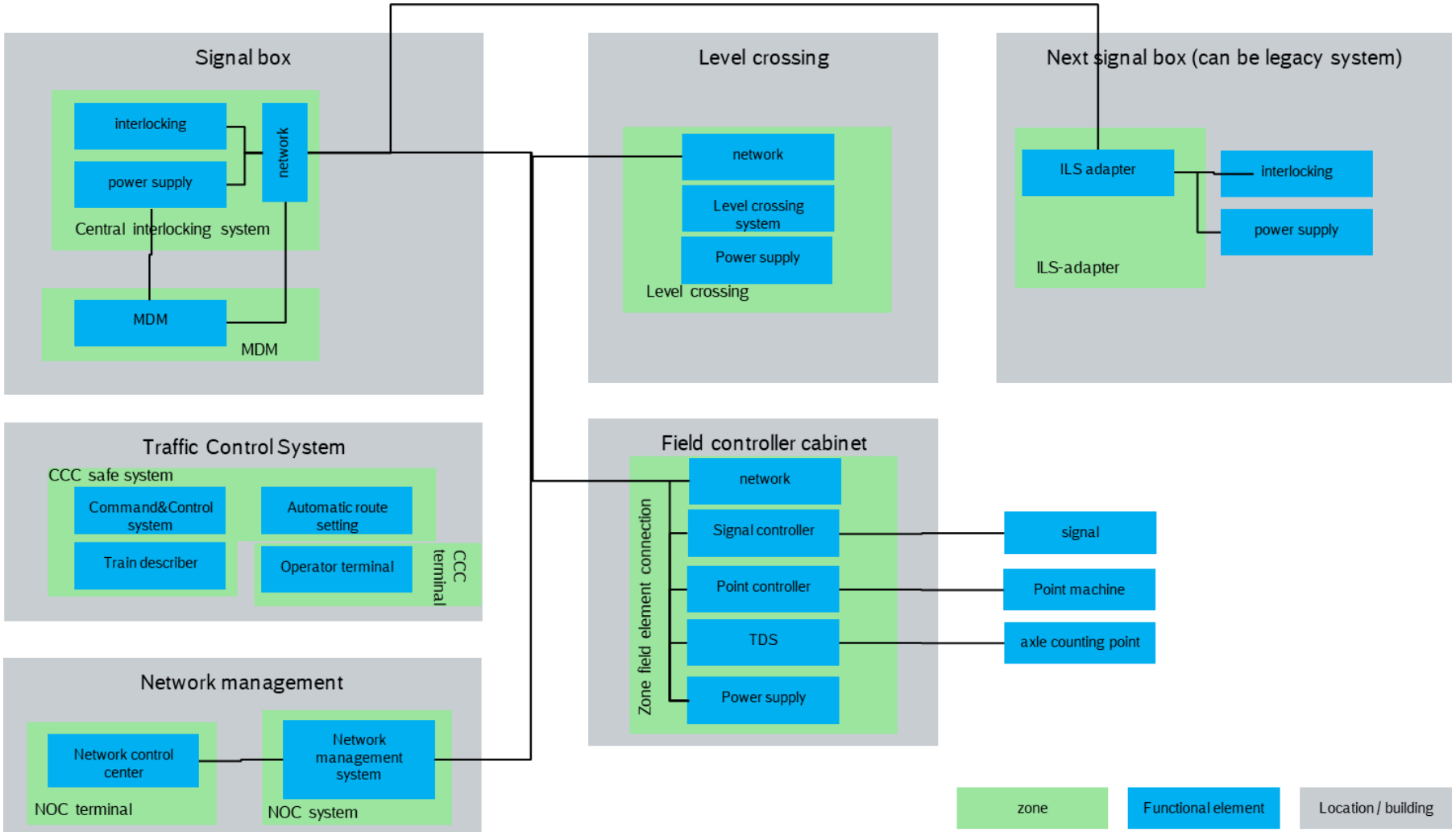

Figure 10 EULYNX Zones 1

For the walkthrough one of the most relevant data gathering systems is taken into consideration. This is the maintenance and data management system (MDM).

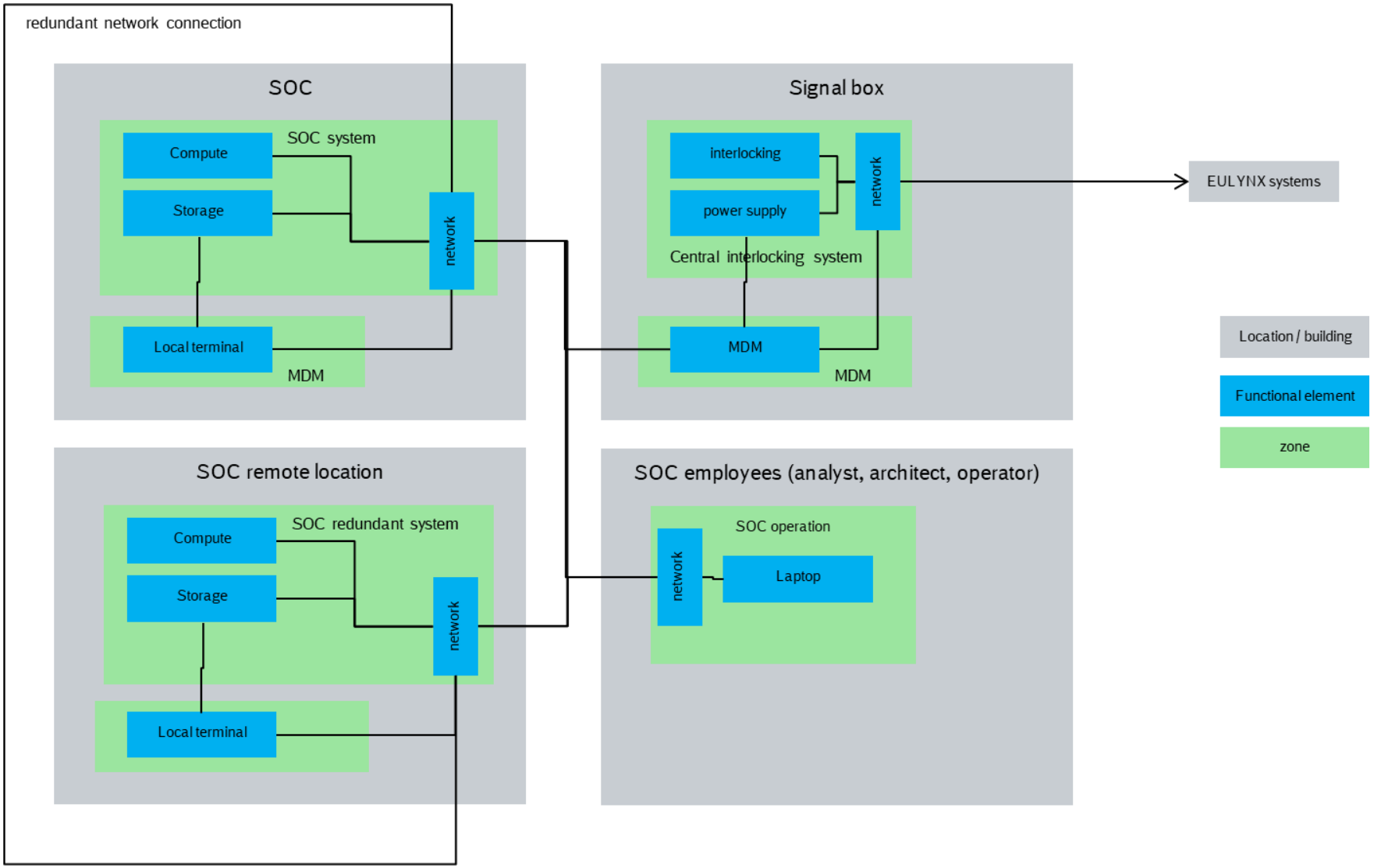

Figure 11 EULYNX Zones 2

The following picture shows the system under consideration.

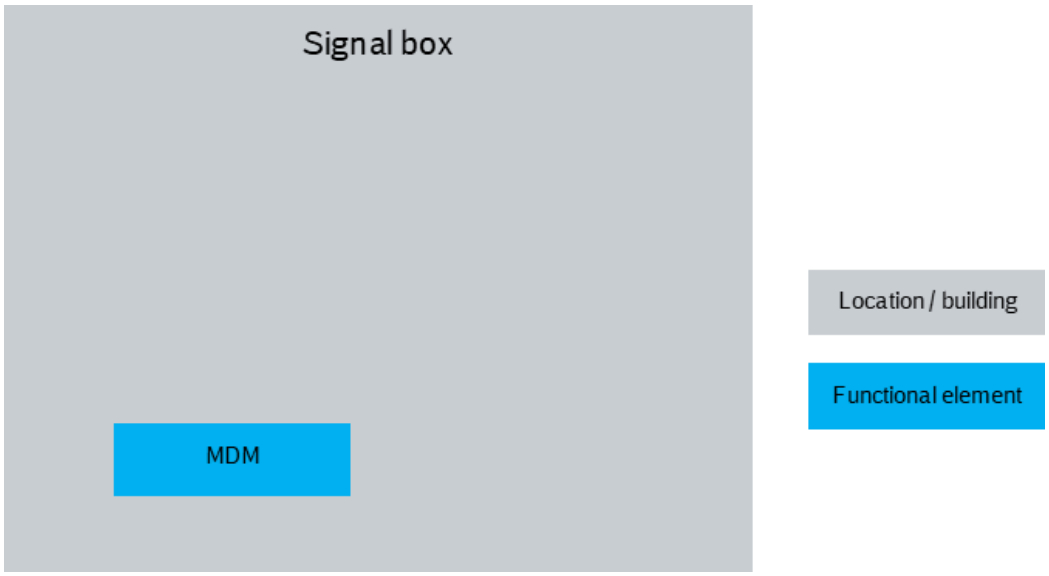

Figure 12 EULYNX SuC Example Zoning 1

In the next step the initial zoning concept needs to be applied.

5.2 Initial Zoning Concept

Here the initial zoning concept, based on the architecture of the system under consideration is displayed:

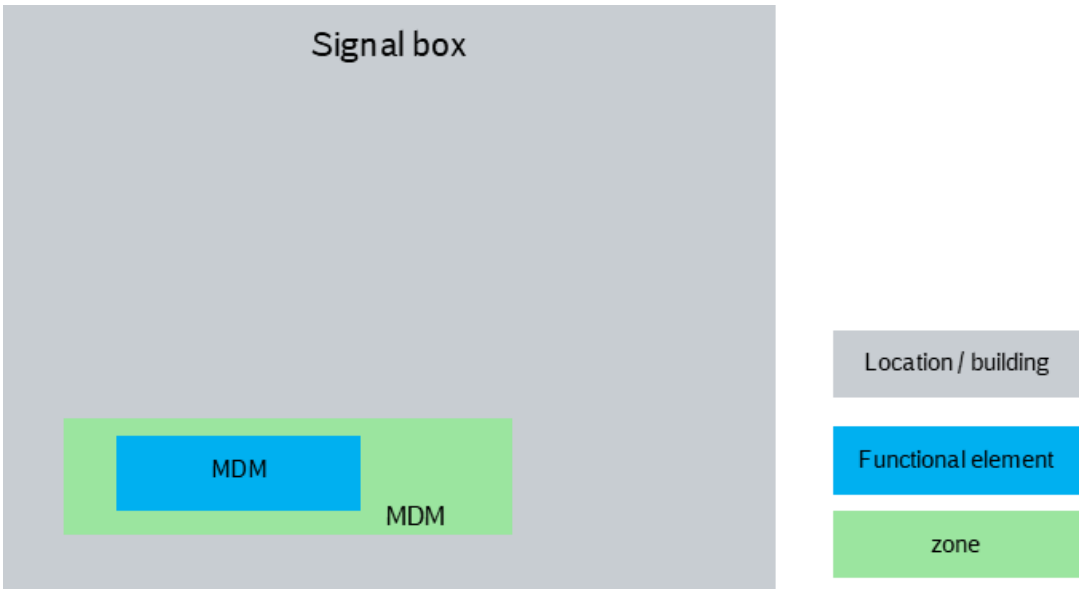

Figure 13 EULYNX SuC Example Zoning 1

5.3 Attacker Definition

In this step, attacker types are identified that might be interested, that threats occur, and which therefore, if realistically considered as causes or triggers for threats could be considered.

Attacker types can be divided into five categories:

a) Intentional, Targeted Attacker (Int)

These are persons who intentionally have a damaging effect on the IT of the C&C system. Targeted attackers are the focus of the analysis.

(b) Human error, untargeted actions (Err)

The C&C system gets attacked this category unintentionally and randomly through mistakes such as operating errors or negligent actions. The system is more likely to damage by accident, mostly by authorized persons.

c) Technical failure (Tec)

In the event of a technical failure, the cause comes from the system itself in the form of malfunctions, and failures. On the one hand, this category focuses on functional safety and resulting risks are mitigated with appropriate measures, on the other hand, it focuses on the availability within the IT security management. The type of attacker is only considered in a limited way.

d) Environmental influences and force majeure (Env)

In this case, harmful environmental factors such as cold or the before mentioned Flash the C&C system . This category is not considered further here since the resulting threats from the basic security measures be controlled.

e) Organizational failures (Org)

This includes insufficient, incorrect, or unclear processes, specifications, or responsibilities.

Following the possible attackers, with respect to the zoning concept and SoC are stated. To easily identify them prTS 50701 recommends putting them in a specific classification. This is especially important for the SOC-process to react to incidents

T.<attack>{<attacker>.<further attributes>}

Since the threat is not known yet, the attacker and further attributes are defined first as:

A.<attack category>.<attacker>.<further attributes>

Further attributes are usually not very helpful to define in more detail. But what will be relevant is the attacker's knowledge and resources for the category of the intentional attackers. The motivation itself is not relevant anymore, since for the group of intentional attackers it is assumed that there is a motivation. Independent from the height of motivation the actual threat that comes from this attacker is defined through capability and resources. So, following process 3b these capabilities are also displayed with the attacker.

		Resources		
		2 Low	3 Moderate	4 Extended
Knowledge	2 General	iSL 2	iSL 3	iSL 4
	3 Specific	iSL 3	iSL 3	iSL 4
	4 Extended	iSL 3	iSL 4	iSL 4

Table 4 Attacker Knowledge and Resources

K = knowledge
R = resources
iSL = initial Security level

- **3a Overall Attacker Type Definition**

A.Int.TerrorOrg

These organizations are made up of radicalized persons, who are drawn from political or religious motives (right-wing, left-wing, Islamist, etc.) carry out targeted attacks and can have extensive possibilities if they have appropriate supporters. Attacks on rail transport may be carried out by Islamist 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 illegal actions such as fraud or extortion to achieve financial goals. They range from small gangs to organized crime (e.g. the mafia). The primary goal is to obtain money. Actions that are designed to simply causing damage are rare with this type of attacker. The following table in rail context is used:

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.

K4

R4

iSL4

A.Int.Comp

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

K3

R3

iSL3

A.Int.Activist

Activists are understood here to be primarily politically motivated attackers who oppose political want to protest conditions and put up a fight. 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 (for example Greenpeace) who do not have detailed information on the internal structure of the railway and do not receive any support from internal offenders. Availability attacks (achieving a blockade) are conceivable, causing security-critical situations (accidents) in which persons are injured do not correspond to their motivation.

K2

R2

iSL2

A.Int.Hacker

A hacker is generally a technically skilled computer user who has a large knowledge of current attack techniques. White-hat hackers are all about penetration into networks and systems and the detection of weak

points, which they cannot use for their own exploit purposes. Black-hat hackers have similar knowledge, but use found weaknesses to enrich themselves financially. Since the behaviour of a black-hat hacker is comparable to that of a cybercriminal, here the white-hat hacker who is not acting on behalf of other organisations.

K3

R2

iSL3

A.Int.Cybercrime

Cybercriminals are IT specialists with criminal energy. They also work by order and out of financial motivation. One example is the blackmailing of companies and authorities (e.g. the Baltimore City Council) by encrypting important or all IT systems and a ransom is demanded for the decryption.

K3

R3

iSL3

A.Int.Malware

This type of attacker is understood to be computer programs that have been deliberately infiltrated, which are executable on the operating system used in the system and predefined have harmful effects. An example are programs that encrypt hard disk contents and only decipher them for a ransom. Malware and viruses differ only in the objectives of their use and are based on technically on the same principles.

K3

R3

iSL3

A.Int.Internal

Internal perpetrators are persons who, as employees or suppliers, have internal knowledge and usually also have IT authorizations and use them to carry out deliberately damaging actions, such as sabotage, betrayal of secrets or infidelity. Internal intentional 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 are not valid anymore, taking into account that access can be easily granted to internal attackers.

K2

R2

iSL2

To reduce the amount of analytic, every intentional attacker type is summed up in the group attacker by taking the maximum identified values and gets the following syntax:

A.Int.Attacker

K4

R4

iSL4

Furthermore, the unintentional attackers need to be displayed. These are less relevant in the capability and especially in the context of MDM and SOC, since only highly qualified personnel is having access to these systems. That is why, they are only summed up here and not described in more detail.

The most critical unintentional attack is done by unintentional virus/malware attacks (e.g. ransomware). The resulting level of this overall group is then:

A.Err.Attack

K3

R2

iSL3

For technical errors it is similar. This type of attacker is the technology itself. The hardware as a necessary component of the technical architecture leads to a threat event. The term Here, "attacker" is to be interpreted in the sense of a technical factor that affects IT security attacks. This type of attacker only refers to the components of the IT security architecture. At all other subsystems / components are exposed to threats resulting from this type of attacker are controlled by the functional safety measures. The metric of knowledge and resources is not applicable in this case. There will be an iSL of 2, because although the failure of a component has negative effects on the availability of the system but does not lead to a danger to life and limb.

A.Tec.Error

iSL2

Organizational errors can be summed up as well. Incomplete, contradictory, unsecure, or faulty processes can be the starting point for security-relevant events but are not themselves an independent threat event. Since at least one further factor must be added for an acute threat, an iSL of 2.

A.Org.Err

iSL 2

- **3c Exclusion of Attackers**

The current example threat analysis shows that governmental organizations and terroristic organizations do not have a major interest in attacking the railway with major cyber-attacks. The theoretical risk of attacks of such organizations in the future is to be mitigated or evaluated in security strategies or business continuity management on organizational level.

Therefore, they are excluded.

Furthermore, the internal, intentional attacker needs a specific treatment. That is why, this category is separated as well. As a result, the following attacker syntax is defined for step 3:

A.Int.Attacker

K3

R3

iSL3

A.Int.Internal

K2

R2

iSL2

A.Err.Attack

K3

R2

iSL3

This assumption might be not feasible for every railway operator, e.g. if the railway operation is considered as critical infrastructure or the threat analysis takes terroristic and governmental organization as likely attackers. When weighing up, it needs to be considered that a SL4 causes much higher security measures, followed by costs over the whole life cycle. This is necessary to set risks and impacts into right relation

5.4 Threat Analysis

Following the relevant threats for the system under consideration, taking the zone concept into account are discussed and displayed. The basis for the threats is a list of known and possible attacks, following today's assumptions.

IEC 62443 sorts them very generic in the foundational requirements. prTS 50701 does not give a hand with specific threats. That is why the catalogue of the BSI (federal organization for information security) is taken as basis and filled up with railway specific knowledge.

In the following it was started with one example for each FR (IEC 62443) to display the full process.

A.Int.Attacker.Unallowed_Access

An intentionally acting attacker logically overcomes the system boundary of the signal box from the outside and creates unauthorized access to the physical object or to logical components (e.g. network, subsystem, C&C system application) about weak points, such as:

- Unsecure / insufficiently secured IP communication / interfaces
- Unprotected or insufficiently protected communication interfaces
- Incorrect or carelessly configured access control
- Options for bypassing firewall rules

Resulting iSL: 3

A.Int.Attacker.Get_Admin_Rights
A deliberately acting attacker gains privileged authorizations (administrator-rights) and uses the following procedures to do so:

- It crashes tools that were started with admin rights
- He uses social engineering

Resulting iSL: 3

A.Err.Employee.Wrong_Usage

An unintentionally acting employee carries out incorrect operating actions and changes unwanted data of a system. There are several vulnerabilities that may underlie this threat, including negligence or carelessness on the part of the employee, but also incomplete, outdated, or faulty documentation.

Resulting iSL: 2

A.Int.Attacker.spy_out

A deliberately acting attacker spies on data and thus brings information unauthorized in experience. For this purpose, he uses different approaches, such as:

- Listening to or recording communications of relevant data the system gets or sends
- Penetration attempts into systems (e.g. brute force attacks)
- Application of exploits

Resulting iSL: 2

A.Int.Attacker.Data_suppression

A deliberate attacker

- falsifies logging data so that no alarm is triggered

- interrupts / prevents the transmission of messages and alarms
- disables alarm devices

and thus, ensures that a delay in the transport of messages via the communication system occurs or messages/alarms are completely prevented.

Resulting iSL: 2

A.Int.Attacker.Prevent_Preservation_Evidence

A deliberate (intentional) attacker

- Covers his tracks by deleting logging data
- Manipulates / deactivates logging devices
- Distorts logging data
- Is not clearly identified

to complicate the response to a security incident and covering traces.

Resulting iSL: 3

A.Int.Attacker.Hardware_failure

The function of a hardware component or a supply system / network is cancelled:

- A technical failure leads to hardware failure
- Lack of resources leads to maintenance deficits and failure
- The hardware is brought to failure by sabotage
- This results in a hardware loss and thus in a hardware failure

Resulting iSL: 2

A.Int.Err.Employee.Unusability

Services or functions of subsystems / components are no longer usable.

- As a result of a malfunction, functions are unintentionally deactivated or locked.
- The system enters an unintended operating state (e.g. due to overload),
- Whereby functions can no longer be used.
- Missing technical or organizational functionalities prevent that in case of a malfunction
- An orderly operating condition can be restored.

Resulting iSL: 2

5.5 Threat Mapping to the foundational Requirements

The mapping on foundational requirements helps to define the iSL (initial Security Level) for each vector. The vector iSL is defined by the standard process following IEC 62443 and prTS 50701.

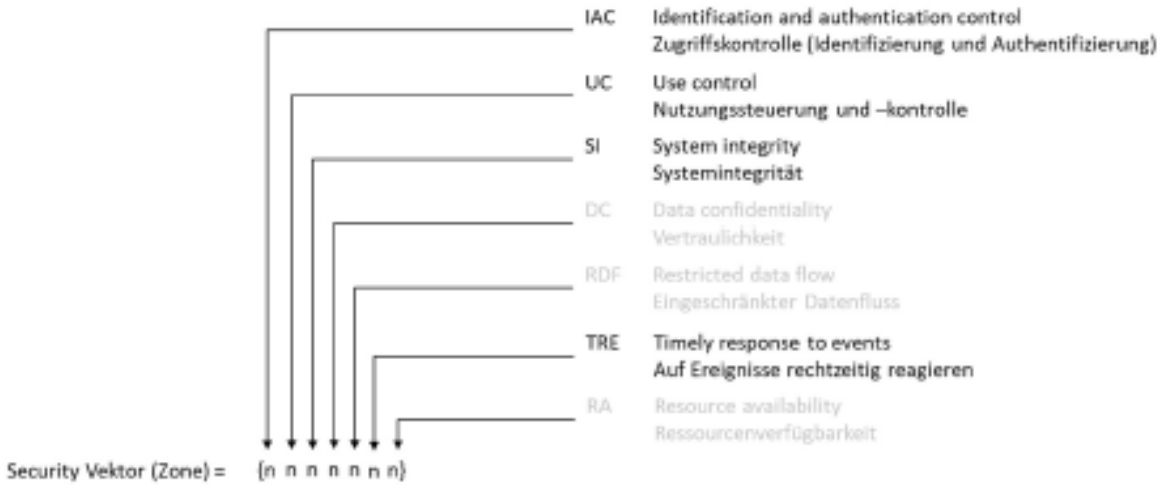

Figure 14 Mapping to Requirements

In the following the threat examples of step 4 are sorted to the FR, so each threat can be mirrored to a vector in the next step. Therefore, the logical of the syntax is widen to:

T.<FR>.<attacker>.<Attack>
T = Threat
FR = Foundational Requirement, to sort it
Attacker = the attacker type
Attack = the actual attack type accomplished

IAC: Identifcation and authentication control

T.IAC.Attacker.Unallowed_Access
Resulting initial Security Level for IAC:
iSL 3

UC: Use control

T.UC.Attacker.Get_Admin_Rights
iSL 3

SI: System integrity

T.SI.Err.Wrong_USage
iSL 2

DC: Data confidentiality

T.DC.Attacker.Spy_out
iSL 3

RDF: Restricted data flow
T.IAC.Attacker.Data_supression
iSL 3

TRE: Timely response to events
T.TRE.Attacker.Prevent_Preservation_Evidence
iSL 3

RA: Resource availability
T.RA.Error.Unusability
iSL 2

5.6 Define initial Security Level per Zone

The aim of this step is to define the final iSL for each zone. Therefore, steps 6a to 6d are performed.

- **6a: Sort relevant Threats to Zones**

In this step for each zone of the system under consideration the relevant threats are listed.

For the MDM-zone the following threats are relevant:

- T.IAC.Attacker.Unallowed_Access
- T.UC.Attacker.Get_Admin_Rights
- T.SI.Err.Wrong_USage
- T.DC.Attacker.Spy_out
- T.IAC.Attacker.Data_supression
- T.TRE.Attacker.Prevent_Preservation_Evidence
- T.RA.Error.Unusability

- **6b: Definition of iSL per FR by the maximal SLs of the threats sorted to the FR**

In this step for each FR the maximum value of the relevant threats sorted is the resulting iSL for the FR:

- IAC - 3
- UC - 3
- SI - 2
- DC - 3
- IAC - 3
- TRE - 2
- RA - 3

- **6c: Put FR Value in Vector of preliminary Zone**

In this step the resulting iSL per FR per zone are put in the zone vector:

Resulting vector, the zone MDM:

Security vector (MDM) = (3 3 2 3 3 3 2)

- **6d: Maximum Value in vector defines**

Now the maximum of the Security vector (zone) is taken and displayed per zone:

The resulting initial security level for the zone MDM is:

iSL (MDM) = 3

- **6e: Use reduction Factor to determine final SL**

In the last step reducing factors can be applied to each zone. Therefore, the following factors can be used. The reason to use this reducing factor is that the IM can evaluate the actual attacker surface or special circumstances to reduce costs, complexity or improve maintainability. Therefore, the reduction is based on rules to support this evaluation.

Not only the strength of the attacker is important for the threat, but also what situation in the attacked zone. Three factors are considered for this: the place of attack, the possibility of damage limitation and criticality of the extent of damage. For each factor is first assumed to be zero (0) and then it is checked whether the threat-mitigating circumstance (see list below) is fulfilled and the provisional

Security Level can be reduced according to the following aspects:

a) Place of attack (LOCATION):

   The value 1 is assigned if the zone cannot be attacked remotely and therefore an Attacker must physically penetrate the zone in order to carry out an attack on railway premises or within railway buildings.

b) Possibility of damage control (POSTRA

   The value 1 is assigned if the zone offers the possibility of an early detection and thus contain the damage or safely identify the attacker and thus to assert claims for damages.

c) Criticality of the extent of damage (POT)

   The value 1 is assigned if an attack in this zone cannot directly cause dangerous damage to railway operations (for example a train accident) - that is to say if there are other safety barriers in this zone which must be overcome for there to be an accident. If the railway operation is directly affected but there can be no danger to life and limb, the value 1 is also assigned.

iSL_{final} = iSL- max {LOC, POSTRA, POT}

For the MDM zone the following analysis can be performed:

a) This factor cannot be applied, since the MDM is sending its data through WAN

b) The MDM is in different places that are well secured, but one cannot say that the attacker can be detected in early stage.

c) The loss of information or delay in the MDM does not directly result into in a dangerous damage to railway operations or in the availability of the system. Factor one can be applied.

Therefore, the reducing factor is {0,0,1} and the final iSL is:

iSL_{final} = 3 – max {0,0,1} = 2

5.7 Apply Security Measures

Based on the initial Security Level (iSL), defined per zone, the necessary security measures are defined and applied to the system.
The result of this phase is a full security concept, that is based on the initial architecture of the system under consideration (SoC), the initial zoning concept and with that initial definition of the required security level.

Threat	Generic Term IEC 62443-2-4	Sub Term IEC 62443-2-4	Measure according to IEC 62443-2-4
T.IAC.Attacker. Unallowed_Access	Workstation → Access to Interlocking / Central Computing Unit	Access Control	The service provider must be able to support multi-factor authentication for workstation computers within the "automation solution" depending on the operator's specifications. This requirement only applies to the workstation computers for which the service provider is responsible.
T.DC.Attacker.Spy_out	Data Protection	Data worth protecting	The service provider must be able to ensure that within the "automation solution" data storage points and data flows that must be protected as defined or confirmed by the operator are documented, including the IT security requirements for their protection (e.g. confidentiality, Integrity).
T.TRE.Attacker.Prevent_ Preservation_Evidence	Data Backup	Execute	The service provider must have the ability to ensure that the "automation solution" is backed up in accordance with the operator's data backup schedules and their goals for data recovery and disaster recovery.

Table 5 Threats and Measures

The Measure-Planning shows that direct measure taking from IEC 62443 does not fulfil requirements to get a railway applicable solution

That is why the table needs to be widened to railway specific measures, meeting the formal requirements on one hand, and can be applied to EULYNX, OCORA and RCA on the other hand.

Threat	Generic Term IEC 62443-2-4	Sub Term IEC 62443-2-4	Railway Specific Application
T.IAC.Attacker. Unallowed_Access	Workstation → Access to Interlocking / Central Computing Unit	Access Control	Physical access to MDM needs to be restricted by personal ID and physical lock. System access to MDM needs to be restricted by personal access / admin access. Unallowed access tries need to be registered by central logging instance with automated reaction, e.g. SOC
T.DC.Attacker.Spy_out	Data Protection	Data worth protecting	Network Access Control in the network management Encryption needs to be applied Unallowed access tries need to be registered by central logging instance with automated reaction, e.g. SOC
T.TRE.Attacker.Prevent_ Preservation_Evidence	Data Backup	Execute	Automated Data Recovery Solution from the MDM Data that can be restored in short time. Automated Data Recovery Solution in different system from MDM logs to allow immediate analysis when anomalies or system break down occurs → SOC

Table 6 Threats - Railway Specific Application

5.8 Risk Assessment

After the security concept is fulfilled with step 7, a risk analysis is needed to be performed on the system. The risk analysis takes into consideration the controls and checks if the applied security measures (techniques, processes) meet the requirements (controls). Untreated risks will also be visible. Each threat risk needs to be assessed with the following aspects:

- Definition of the target risk (usually “low”) **-> Low**
- Evaluation of the actual risk by using the following steps and calculations:
  - > Evaluation of the exposure of the system **-> 2**
  - > Evaluation of the Vulnerability of the system **-> 2**
  - > The result is calculated to a likelihood **-> 3**
  - > Evaluation of the Impact of a fail or manipulation of the system **-> C**
  - > In the end the combination of likelihood and threats causes a risk. **-> Significant**
- Evaluate risk delta **-> 2**

  (In this case, compensating measures needs to be performed)
- Measures from IEC 62443 **-> ID 42** (Alert personnel during system failure)

  Risk Assessment

  - > Evaluation of the exposure of the system **-> 2**
  - > Evaluation of the Vulnerability of the system **-> 2**
  - > The result is calculated to a likelihood **-> 3**
  - > Evaluation of the Impact of a fail or manipulation of the system **-> C**
  - > In the end the combination of likelihood and threats causes a risk. **-> Significant**
- Evaluate risk delta **-> 2**

  (In this case, compensating measures needs to be performed)
- Compensation Measures **-> Debug Logging, -> Testing Procedures**

  Final Risk Assessment

  - > Evaluation of the exposure of the system **-> 1**
  - > Evaluation of the Vulnerability of the system **-> 2**
  - > The result is calculated to a likelihood **-> 2**
  - > Evaluation of the Impact of a fail or manipulation of the system **-> B**
  - > In the end the combination of likelihood and threats causes a risk. **-> Low**

The Security measures for this example are powerful enough to reduce the actual risk from medium to the final risk low. No additional risk acceptance explanation is necessary in this case.

Example:

Threat catalogue	FR - 5	MDM	Target Risk	Exposure	Vulnerability	Likelihood	Impact	Actual Risk	Risk delta	Measures from 62443	Exposure	Vulnerability	Likelihood	Impact	Actual Risk	Risk Dela	…
T 026 Malfunction of Devices or Systems	IAC	Relevant	Low	2	2	3	C	Significant	2	ID 42	2	2	3	C	Significant	2	…

…	Compensation Measures	Exposure	Vulnerability	Likelihood	Impact	Actual Risk	Risk Acceptance Delta	Risk Acceptance Explanation	Explanation
…	Debug Logging …	1	2	2	B	Low	0	/	Assumption: failure of devices could cause …

Table 7 Risk Assessment Example

If there are risk that are not treated or mitigated, there are three possible solutions:

1. Adjust the security measure for the zone. This is then a feedback to step 7, as also shown in the overall process picture
2. Name a mitigation and add this to the documentation of the security concept. This is also a feedback to step 7.
3. Accept the risk. In this case the risk acceptance and the reason for accepting or the possibility to accept it, needs to be documented.

This analysis can only be performed at the system design itself.

6 Appendix

6.1 EULYNX_RCA_OCRORA_Risk_Assement_Calculation.xlsm

EULYNX_RCA_OCOR
A_Risk_Assessment_

6.2 Security Engineering Process Example: smartrail4.0

The following figures and tables illustrate the interaction between EN 50126 and a security engineering process completely.

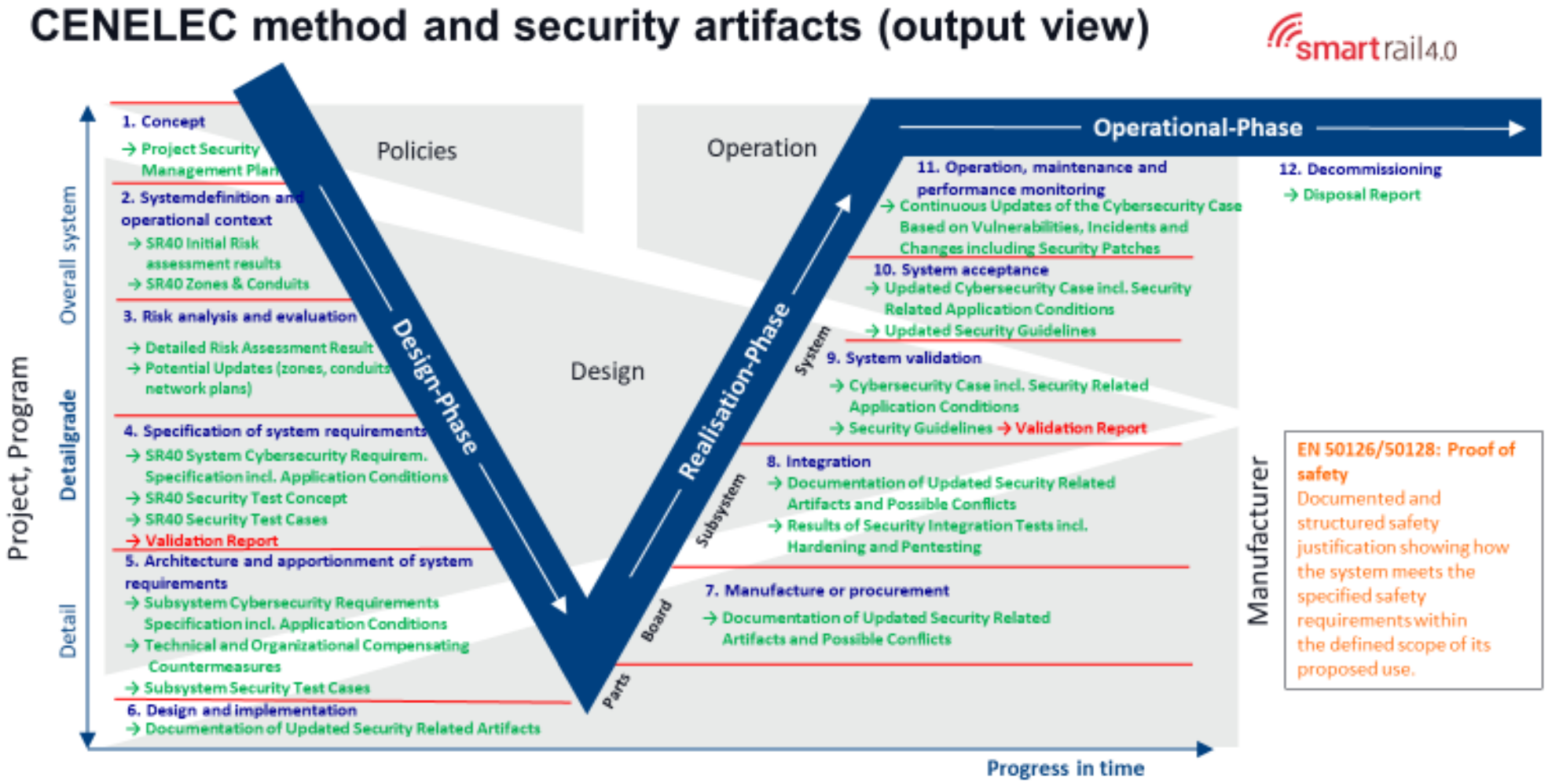

Figure 15 Example of a CENELEC V-Model mapped with Security Interaction

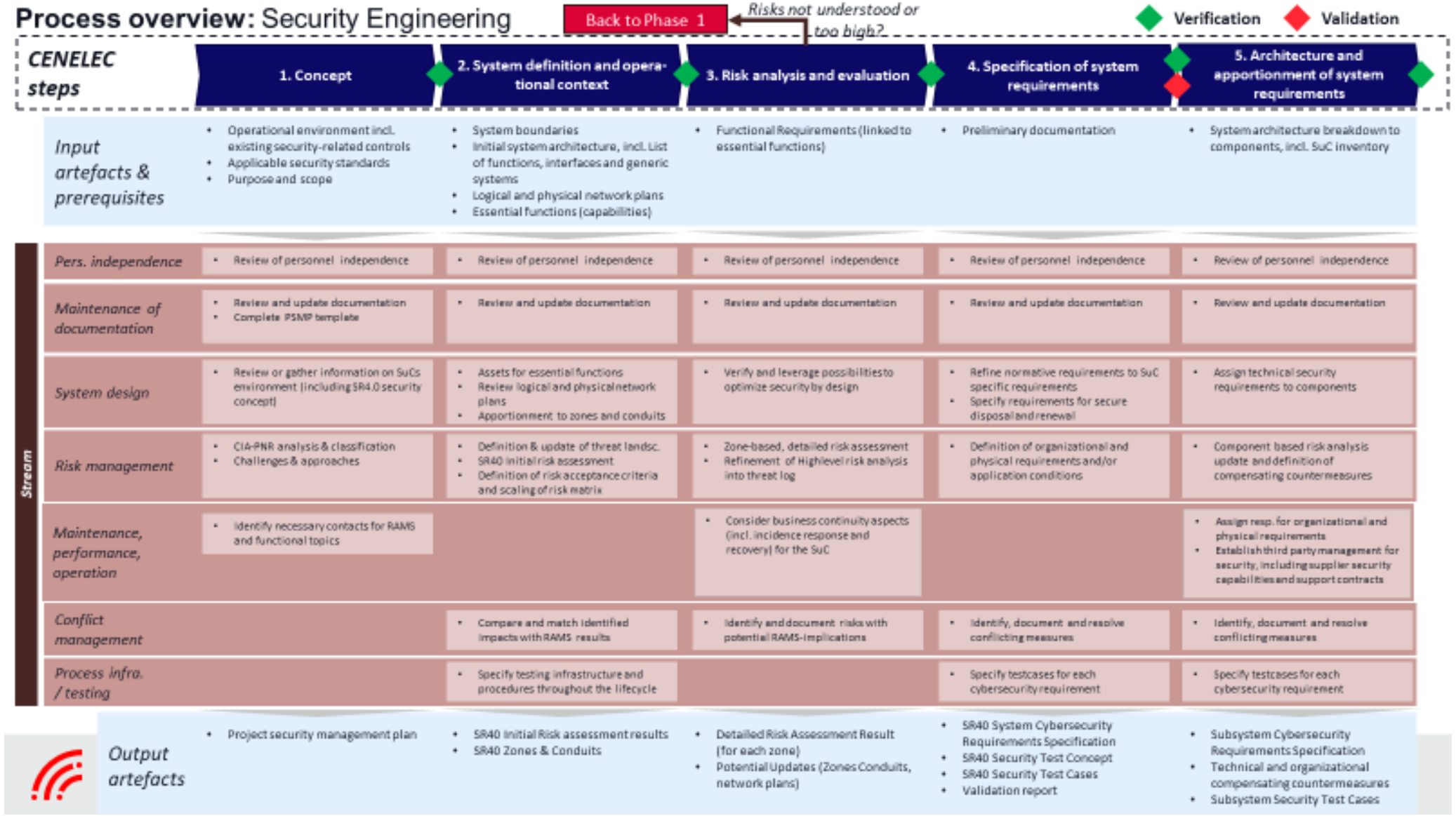

Figure 16 Example of a CENELEC Phase Model Phase 1 - 5

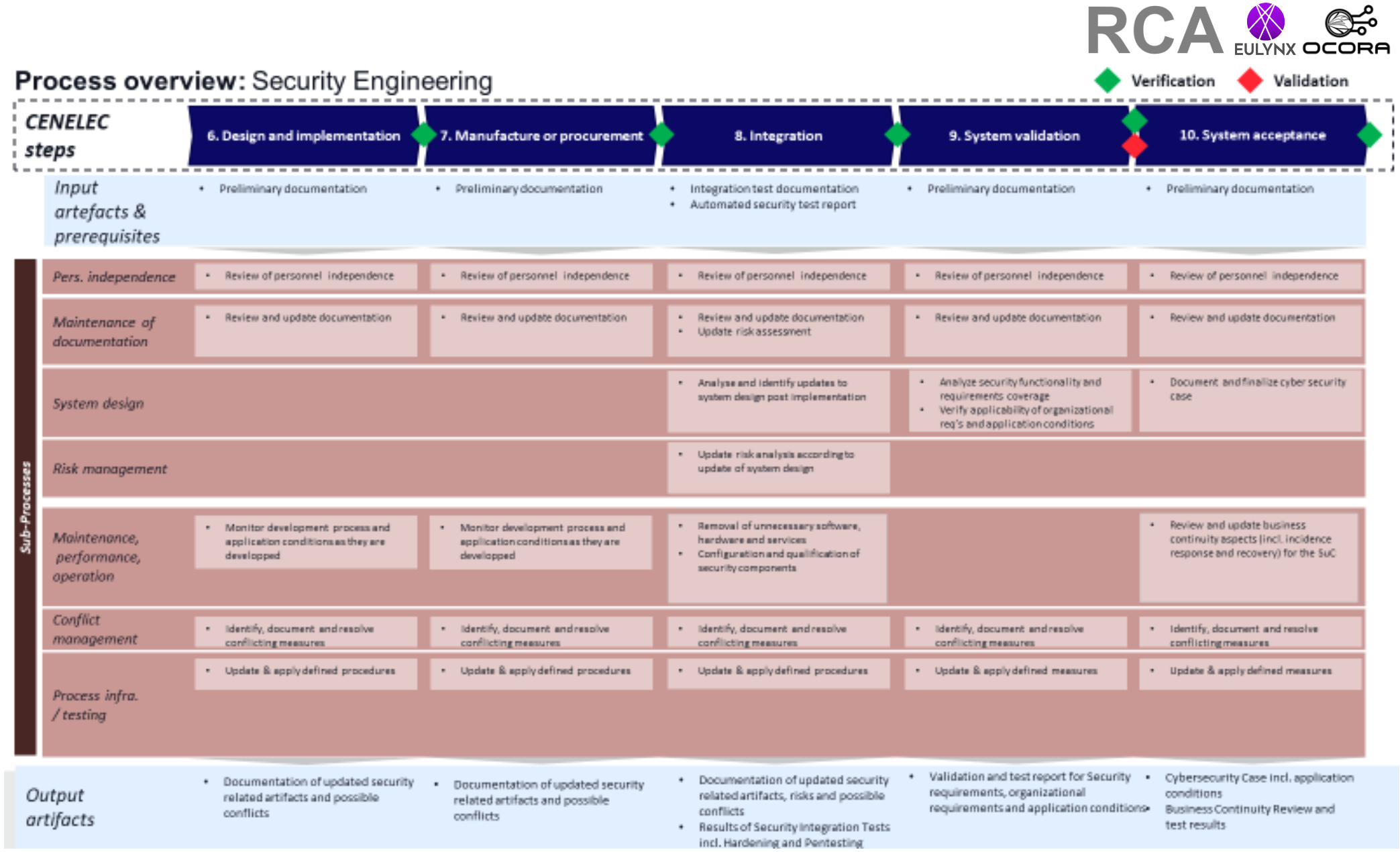

Figure 17 Example of a CENELEC Phase Model Phase 6 - 10

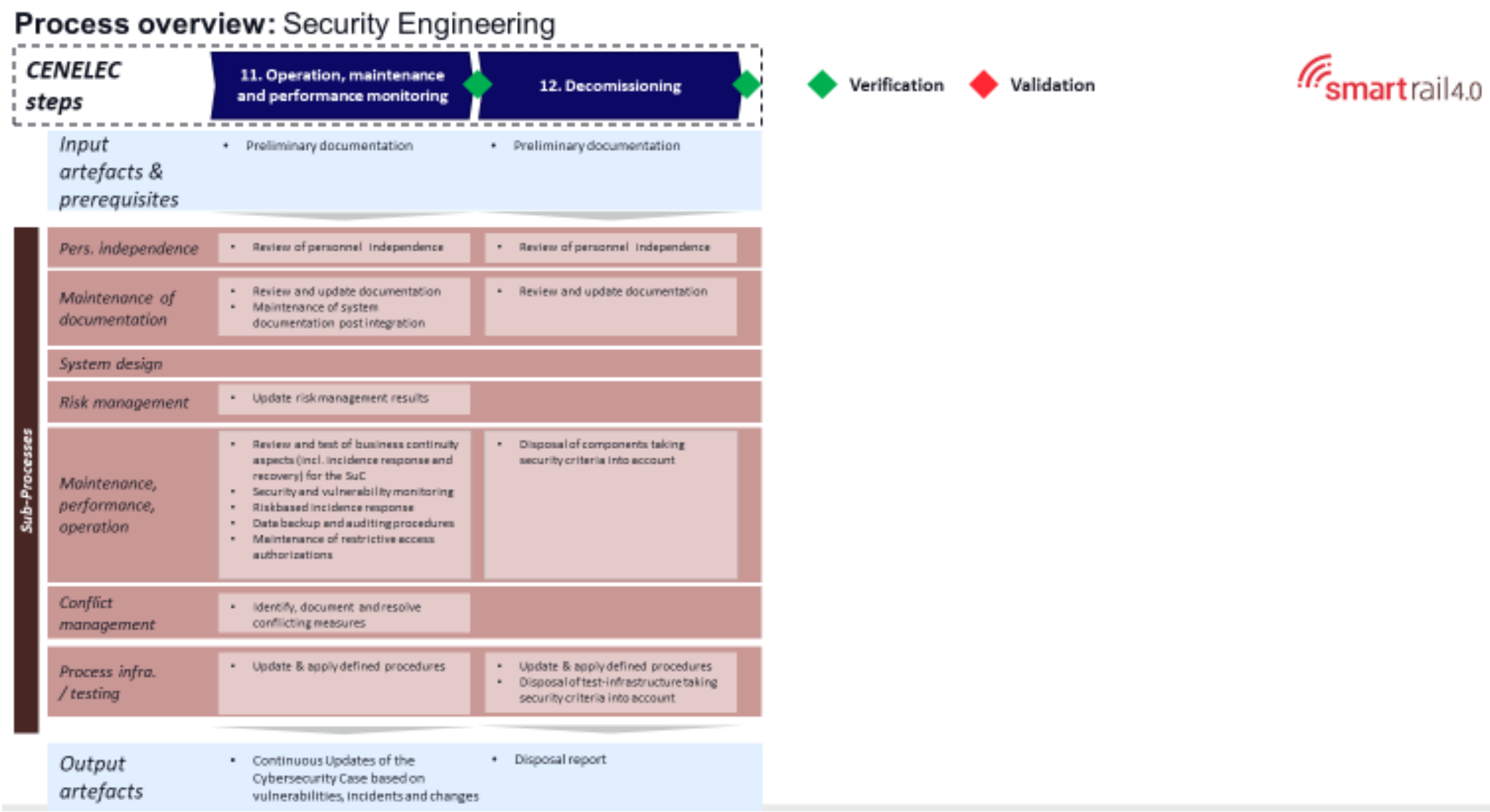

Figure 18 Example of a CENELEC Phase Model Phase 11 - 12

END OF DOCUMENT