enisa

European Rail ISAC

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ZONING AND CONDUITS FOR RAILWAYS

FEBRUARY 2022

ABOUT ENISA AND ER-ISAC

The **European Union Agency for Cybersecurity, ENISA**, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

The **ER-ISAC** is an initiative driven by the European Rail Infrastructure Managers and Railway Undertakings. ISAC stands for Information Sharing and Analysis Center and is a community of Information and cybersecurity experts that has a strong focus on the Cybersecurity of Industrial Control Systems and related IT Infrastructures. The Community is a Public and Private partnership that shares various degrees of Cybersecurity information valuable to the entire Rail transport sector. The mission of the European Rail ISAC (ER-ISAC) is to improve the resilience and security of its members, European Rail Infrastructure Manager and Railway Undertakings and its partners. This is done through effective information sharing and by engaging expertise from many types of functions in joint efforts for the analysis of threats, vulnerabilities, incidents, solutions and opportunities. ER-ISAC offers a community of communities to facilitate this proactive information sharing and analysis, allowing its members to take their own effective measures. The ER-ISAC would like to express their gratitude for the support of the UIC - International union of railways. More information about the ER-ISAC and its work can be found here: https://er.isacs.eu/

CONTACT

To contact the authors please email info@enisa.europa.eu
For media enquiries about this paper, please email press@enisa.europa.eu.

AUTHORS

Klarer Helmut, ÖBB
Christian Schlehuber, Cybershield Consulting

EDITORS

Klaasjan Ooms, NS
Marianthi Theocharidou, Rossen Naydenov, ENISA

CONTRIBUTORS

Lies Alderlieste, NS
Davide Amato, SADEL
Omar Benjumea, Selectron
Atillio Ciancabilla, Ferroviaria Italiana
Jasmin Cosic, Deutsche Bahn
Yseult Garnier, SNCF
André Shant Hagope Khatchik, Infraestruturas de Portugal
Giulio Magnanini, Ferroviaria Italiana
Andreas Meyer, Selectron

Tristan Moreaux, SNCF
Quentin Rivette, SNCF
Francesco Sperotto, Hasler Rail
Gertjan Tamis, NS

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-571-5 doi 10.2824/761090 Catalogue Number TP-06-22-138-EN-N

TABLE OF CONTENTS

TABLE OF FIGURES

EXECUTIVE SUMMARY

This document gives guidance on building zones and conduits for a railway system. To do so, first the methodology is described. This approach is based on the recently published CENELEC Technical Specification 50701 (CLC/CLC/TS 50701:2021). The approach is complemented with additional practical information and hints on how to make the implementation of zoning easier for a railway operator. It gathers the experience of the European Railway Information Sharing and Analysis Center and its members, i.e. European infrastructure managers and railway undertakings.

Each of the steps of the zoning process is explained in detail. The document shows what standards are required in each step and what processes should be performed. Additionally, the document discusses the documentation that should be created during each step and guidance in the form of a 'cookbook' is given.

During the zoning process, zoning models are developed over three iterations:

1. "Proposal railway zoning model": it is used in the first steps, ranging from first collecting information and designing initial zones (ZCR 1) up to the stage where zones, conduits, communication lines and security levels (SL) get verified briefly for the first time (ZCR 3). The proposal zone model is generic. It can be aligned with but need not fit the corporate structure.
2. "High-level railway zoning model": it contains a concrete and defined risk verified architecture (ZCR 4) and is implemented via cybersecurity measures (ZCR 5). The company specific high-level zone model should be orientated to the corporate structure.
3. "Final railway zoning model": it is a detailed and verified version of the high-level model, reflecting the corporate structure within all zones, conduits and communication lines, the SL ZC and other information (ZCR 6 to ZCR 7).

At the end of this document, the phases after zoning is complete are discussed, i.e. Migration (ZCR 8) and Operation (ZCR 9). Finally, the issue of legacy systems is commented on briefly.

ACRONYMS

ATP automatic train protection

CISO chief Information security officer

CRS cybersecurity requirements specification

CVE common vulnerabilities and exposures

DRA detailed risk assessment

DMZ demilitarised zone

DoS denial of service

ENISA European Network and Information Security Agency

ERA European Railway Agency

ER-ISAC European Railway Information Sharing and Analysis Center

ERTMS European Rail Traffic Management System

ETCS European Train Control System

EU NIS European Union Directive on Security of Network and Information Systems

EVC European Vital Computer

HVAC heating, ventilation and air-conditioning

IACS industrial automation and control system(s)

IEC International Electrotechnical Commission

IoT internet of things

ISO International Organization for Standardization

IT information technology

IXL Interlocking

LAN local area network

NIST [US] National Institute of Standards and Technology

OT operational technology

SCADA supervisory control and data acquisition

SL security level

SL-A achieved security level

SL-C capability security level

SL-T target security level

SR system requirement

SuC system under consideration

TS technical specification

ZCR zone and conduit requirements

1. INTRODUCTION

This document gives the reader additional guidance on the topic of zoning and conduits in the railway sector. This topic is introduced in a general way in the standard series IEC 62443, as well as CLC/TS 50701:2021. The concepts from these standards are used as a foundation and their application is explained in more detail. This document contains an initial chapter, which provides an overview on the topic of zoning and conduits. Afterwards, each step of the process is explained in detail. Each of these process steps is described as follows.

- At the beginning a guiding question is defined, which aims at explaining to the reader why this activity must be performed and what the expected outcome might look like.
- After this, the current step in the process is outlined and the relevant parts of CLC/TS 50701:2021 or the IEC 62443 series are indicated. Should the reader already have some knowledge of this process step, he can skip the subsequent subsections of the chapter accordingly, as these provide detailed guidance.
- Following this, design considerations for the process step are shown.
- Then the section that follows provides detailed guidance on how to perform the step and ensure that the desired results are produced.
- Each section concludes with the identification and explanation of domain specific stipulations, as well as some hints on implementation.

The document concludes with a quick look at the area of legacy systems.

2. ZONING AND CONDUIT METHODOLOGY

The following section gives an overview of the process of zoning and conduit methodology. Each phase is then described in detail in the chapters that follow.

2.1 GENERAL OVERVIEW

ZCR 1: Identify assets and basic process demands:

a) Identify all assets;
b) Create a 'draft architecture' or a 'proposal zone model' following EN62443-3-2 (chapter 'Architecture and Design Principles').

ZCR 2: Identify global corporate risks through an initial risk assessment

ZCR 3: Perform zoning

a) define the basic system context (networks in the company and their criticality, principal communication matrix);
b) define zone, conduits, communication lines and ZC-levels;
c) go from draft or proposal zone model to the high-level zone model (following EN 62443-3-3);
d) define proposals for target security level (SL-T) for each conduit (zone and SuC);
e) establish the high-level zone model by verifying proposal zone model.

ZCR 4: Perform high-level risk assessment with the high-level zone model and the designated SL for exceeding risk

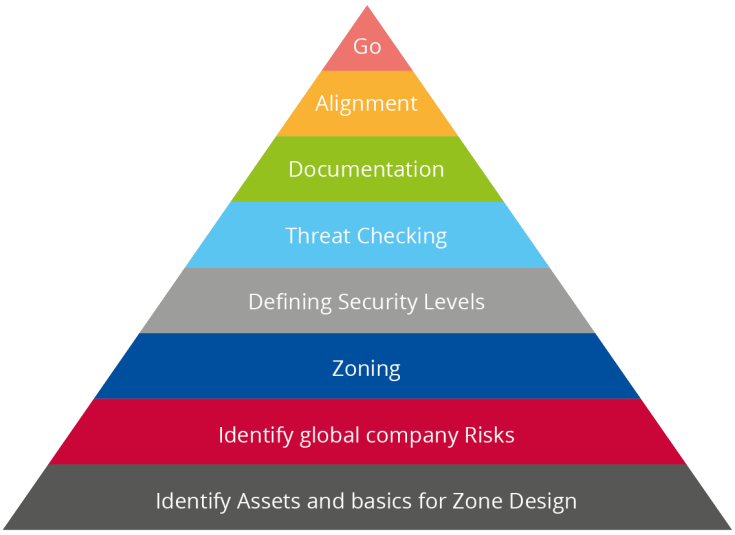
ZCR 5: Check threats

a) Check the high-level zone model against cybersecurity threats.
b) Identify countermeasures (following EN62443-3-3) and modify the high-level zone model to become the final zone model.
c) Verify the 'final zone model' through a detailed risk assessment.

ZCR 6: Document all information and results

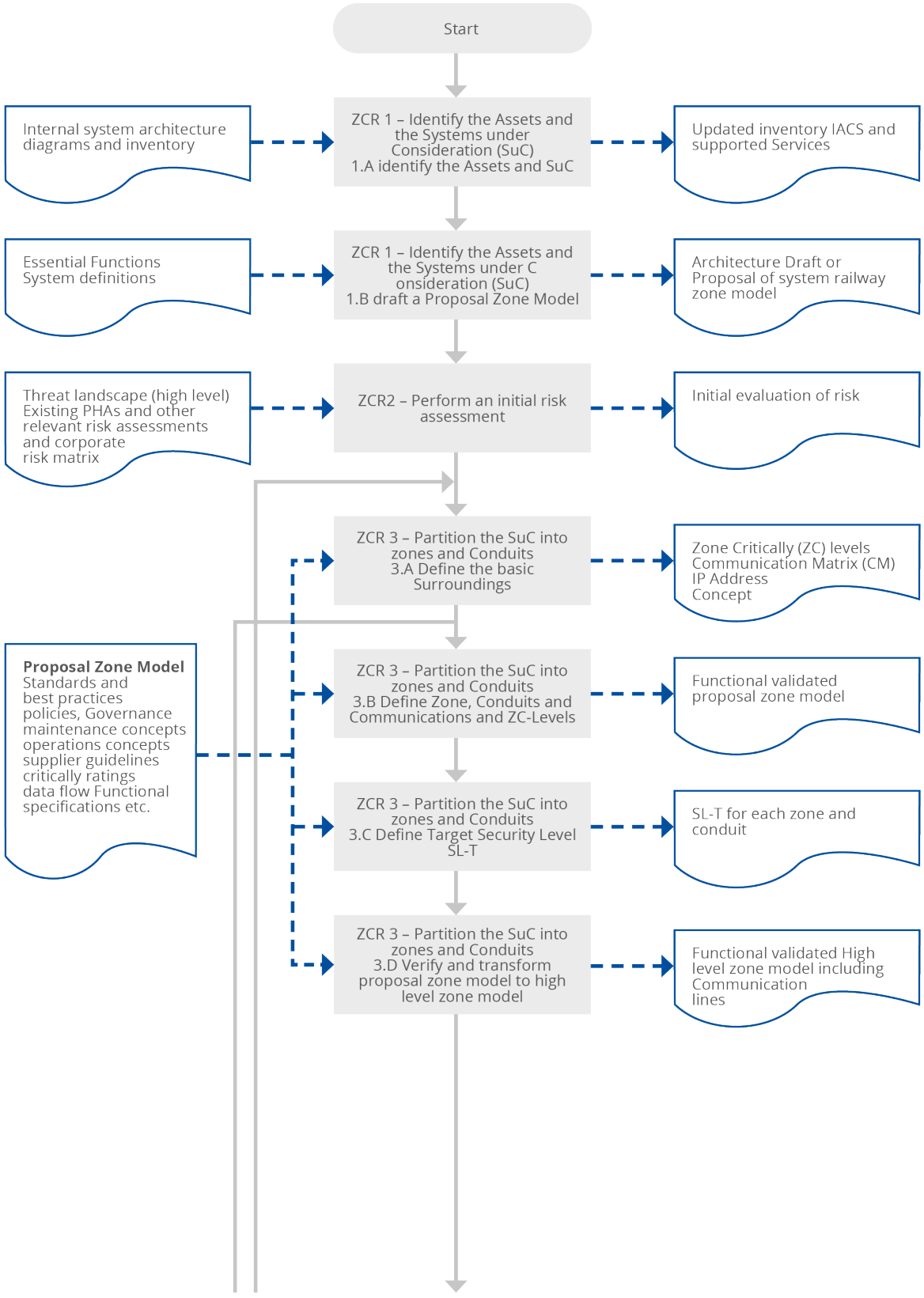
ZCR 7: Get approval from all stakeholders

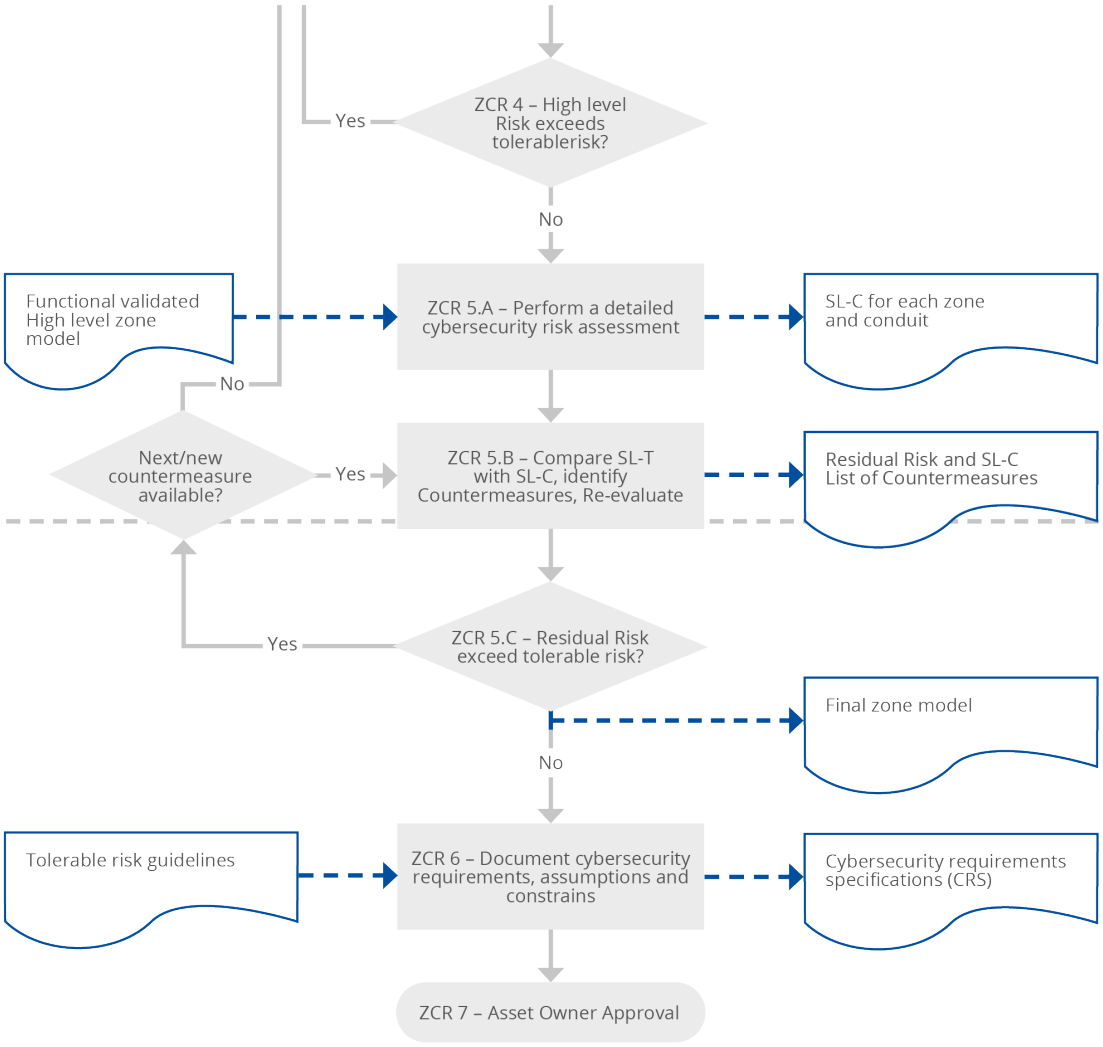
Figure 1 Zoning and conduit methodology



The overall process steps to define zones from scratch based on the standard processes in CLC/TS50701:2021 and EN62443-3-2:2018 are shown below. In this paper, some states are split for easier explanation.

Figure 2 Zoning process: overview





The final zone model depends on existing systems and zones, the result of the threat risk assessment and the target architecture of each railway operator. Security parameters such as security levels (SL), zone criticality (ZC) or protection profiles are discussed in separate chapters and are built upon of this generic base.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ALL CHAPTERS
EN 62443-3-2:2018	ALL CHAPTERS
EN 62443-3-3:2018	ALL CHAPTERS

3. ZONING STEPS

3.1 IDENTIFICATION OF ASSETS AND THE SYSTEM UNDER CONSIDERATION (ZCR 1)

Guiding questions. What assets will be considered? What organisational and technical boundaries exist? Which process standards must they fulfil? What asset groups, lifecycle groups and legacy systems exist? How many employees are working on security?

3.1.1 Process

Figure 3 Identification of assets and SuC (ZCR 1)

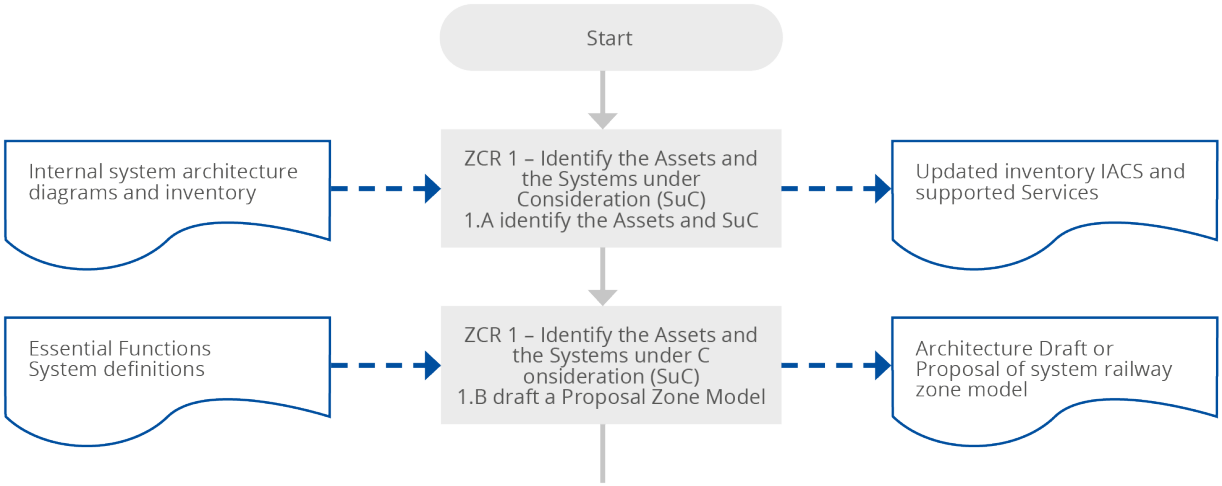


Figure 3 illustrates the steps to be applied to perform the initial risk assessment as a second step and to derive a security architecture in 'zones and conduits'.

3.1.2 Related parts of standards

Overall functional description

The location of the SuC within the model of the railway architecture shows the kind of system to which the SuC belongs (e.g. rolling stock, signalling, infrastructure etc.) and which main functions are supported. The identification of the cybersecurity threat to the SuC should be based on a SuC where the system boundaries and the functionality provided are defined.

Therefore, this identification of the main functions should be detailed by providing information related to:

- the objective (intended purpose) and the mission profile of the SuC comprising the definition of the system functions, the system borders and the interfaces;
- the operational scenarios, which define how the SuC will be used and which actors are interfering or interfacing with the SuC;
- the context of their implementation and use;

- the planned lifetime and therefore, possibly, necessary system updates to HW and SW;
- maintenance plans and concepts for the SuC;
- constraints due to the environment which integrates with the SuC [Source: CLC/TS 50701:2021].

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.2.2

Assets supporting the essential functions

Assets supporting the essential functions of the SuC shall be clearly identified in the definition of the system along with their relationship with their corresponding essential functions. [Source: CLC/TS 50701:2021]

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.2.5

3.1.3 Design information

3.1.3.1 Note for security-architecture in greenfield environments

It is highly recommended that the processes of communication and the process of the essential functions at a high level be checked with the responsible owner of the essential function before going forward to ZCR 2 in order to prevent a re-design of the zone model and thus a step back to ZCR 1 from a later stage.

3.1.3.2 Note for security-architecture in brownfield environments

Should an existing system need to be zoned after it is already in operation, things get a bit trickier. In general, it is advised to undertake zoning in this case in a pragmatic way by implementing the PERA model. This means that two clusters with boundary protection devices (most likely NG-FWs) are applied and a DMZ is built, with a cluster to the north and the other cluster to the south. After that has been done, all 'normal' IT devices are put in a zone north of the DMZ, while all OT devices are put in a zone south of the DMZ. After that, the communication is configured in such a way that no direct communication from IT to OT is possible. Also, depending on the maintenance windows, a more fine-grained approached might be applicable.

Hint: zoning is similar to a puzzle with 10 000 parts. After emptying the box, you turn all the parts bottom down to see the surface. Then you separate and group together the parts such as persons, buildings, walls, background. Sky also a functional grouping such as edge parts or notches. Then you build up the first island, try to locate it in the frame and move the islands to other places as necessary. Lastly, you connect the islands.

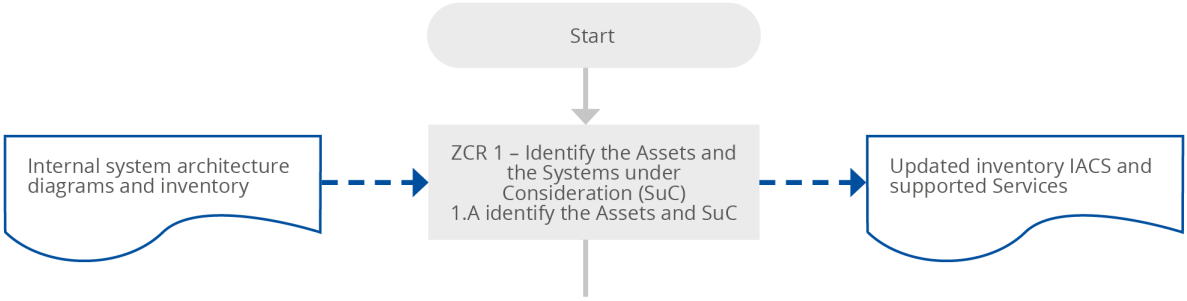
3.1.4 Additional guidance

In this section additional guidance is given. Should you be experienced already with the activities in this step, you can skip this section.

3.1.4.1 Cookbook step 1a: identify assets, communication and SuC

Process

Figure 4 Collecting asset information



Input

All asset and inventory information 'systems' independent of their sources (central IT CMDB, decentralised CMDB, PLC Tools, Excel sheets, etc.)

Hint: well-known PLC vendors often use proprietary asset management systems to check firmware and for device parameter (backups) done by the engineering staff. These industrial or decentralised CMDBs are often not acceptable in the IT environment but they do provide a high actual status concerning many OT devices.

Task

1) Collect all asset information from all entities and departments. After retrieving all this information, check again in order to ensure that nothing has been missed.

Identify:
- all assets, all systems,
- functionality demands,
- entity boundaries,
- interfaces to external companies, RU, IM,
- cloud environments and mobile network connections.

Note: there are more bodies to recover and unique systems to explore than you would ever believe. Should you come across a system for which nobody wants to be responsible, consider whether a system without an owner is desirable in your organisation. Perhaps shutting it down may result in a new owner for the system stepping up.

2) Identify and define organisational or technical SuCs ('entity subsystems'), for example, signalling, energy, office, datacentre, industrial, rolling stock (see Figure 7 or Figure 1

Hint: if all ISE and ISA are supporting the CSA, they can work in parallel and thus speed up the overall process.

Output

High-level documentation of:
- assets and their communication needs;
- asset groups and their critical needs;
- process and organisational or entity boundaries;
- principal communication flow.

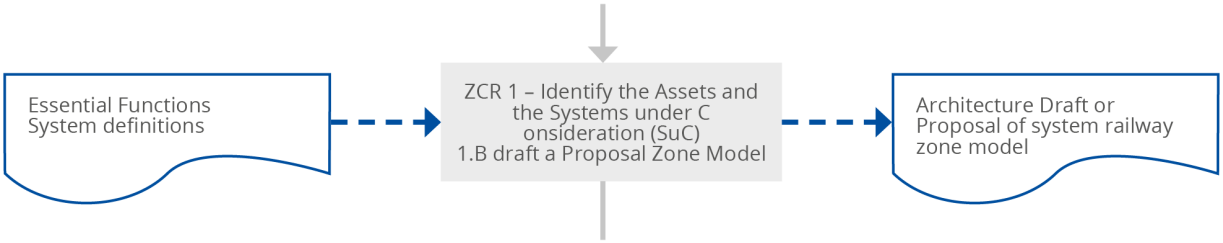
Note: a strong collaboration and support between the CSA and all ISE, ISA, ISO and CISO helps to meet this challenge in a manageable timeframe.

3.1.4.2 Cookbook step 1b: group assets into a 'proposal zone model'

Hint: this step is in general not described in other standards. Grouping assets into a proposal zone model, and especially knowing the boundaries, makes life easier for the high-level assessment of risk that follows.

Process

Figure 5 Proposal zone model with all assets and communication information



Input

All asset, inventory, and communication information is from Step 1.A.

Task

1) The railway operator should define an asset model of its railway system. Assets should be split into groups corresponding to physical areas, entities and levels of functional criticality.
    - Assign the responsible assets to the entity subsystems (signalling: signalling, command & control, auxiliary, comfort, public interlocking, crossing, RBC, switches, etc.)
    - Group the assets and technical SuC into a draft of zones by their essential process functions (energy: power plants, substations, switch heating, tunnel systems, traction mains, etc.).

Hint: look at the 'Railway asset model' chapter.

The resulting model is an input to define the SuC and zones

2) Identify all physical and logical boundaries of the SuC and each process or utility area.
3) Identify all physical and logical points of access to the SuC and each process or utility area.
4) Connect zones and conduits between the zones by their essential process functions in the entity subsystem.
5) Connect the entity subsystems to a corporate model and identify borders ('place for firewalls').
6) Define the critical zone levels and a communication matrix.

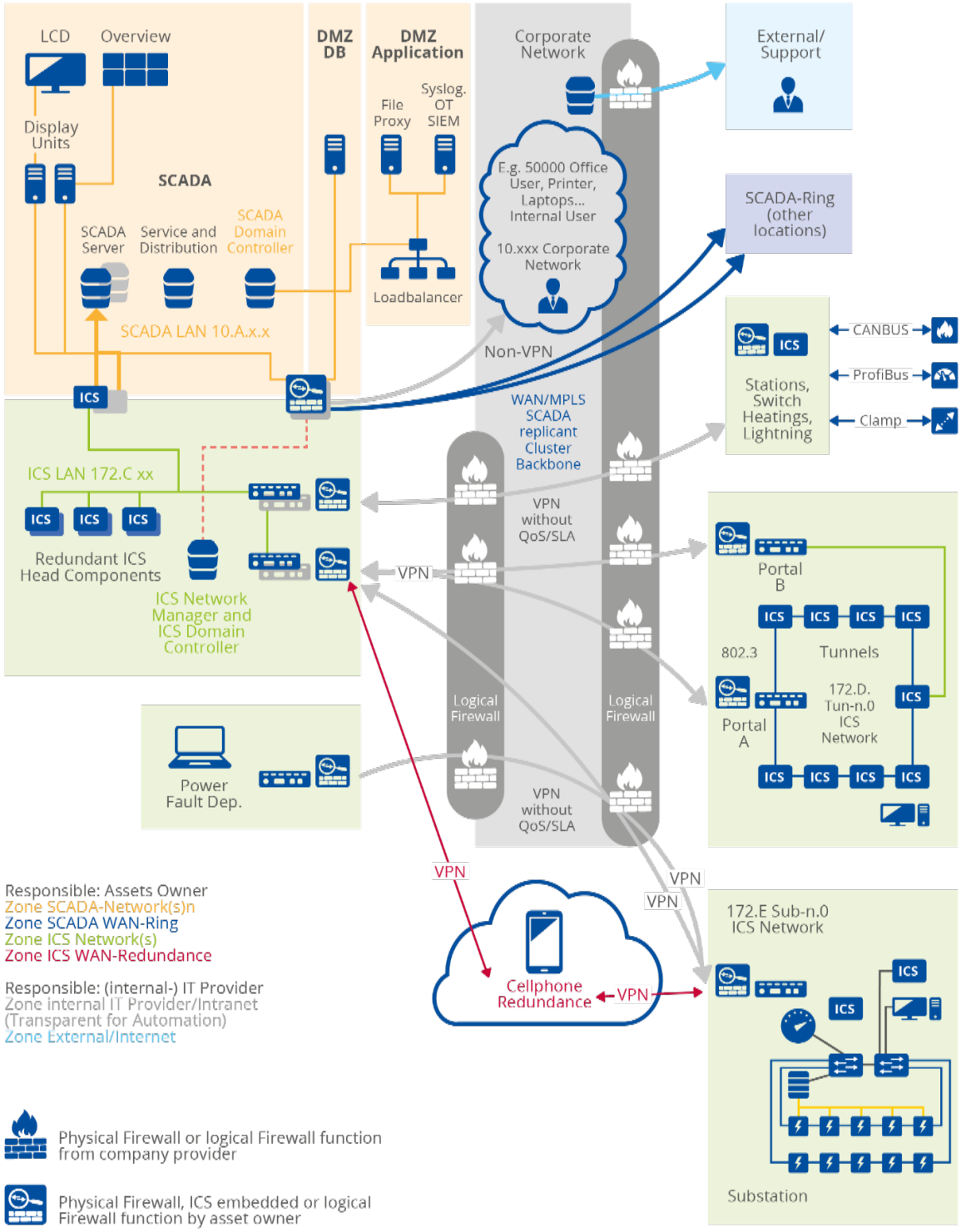
Note: strong collaboration and support between the CSA and all ISE, ISA, ISO and CISO is necessary to overcome this challenge in a manageable timeframe.

Output

- A proposal (of a railway system) zone model (architecture draft) and high-level documentation of:
    - organisational SuC (or subsystem to prevent misunderstandings with technical SuC);
    - zones in the organisational SuC;
    - technical SuC such as interlocking systems or substations;
    - communication scheme at a high level with conduits and boundaries or at least a record of the boundaries and points of access to the SuC and each process;
- A high-level description of the SuC to include the name, a high-level description of the function and the intended usage of the SuC, as well as a description of the equipment or process under control as it is known at the stage of initial risk assessment;
- At a later stage, during the detailed risk assessment, this SuC description should be completed to achieve a detailed description of all assets (reference and version).

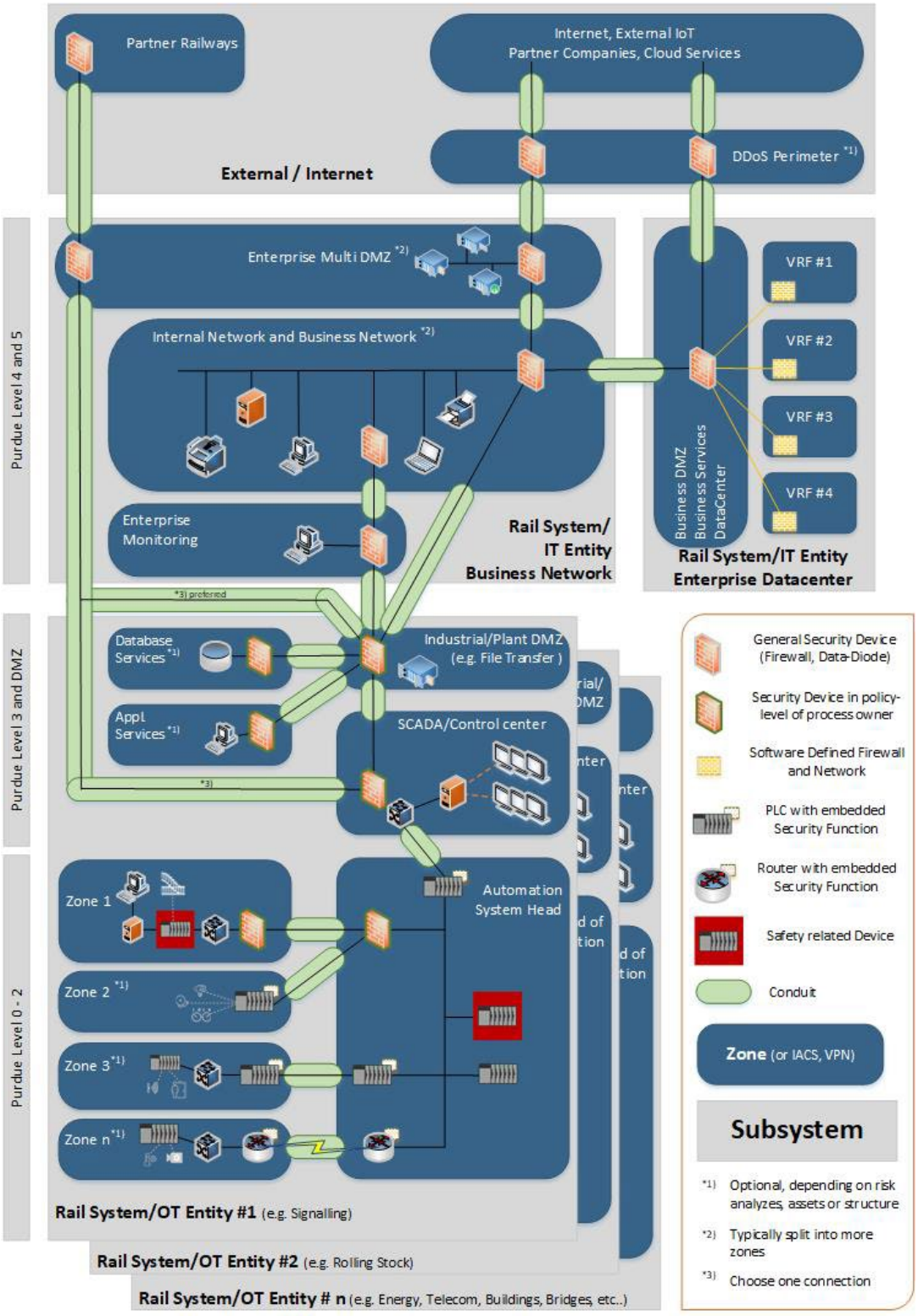
A simplified example for one entity (SuC) including the main ways for communication:

Figure 6 Simplified example of a proposal zone model for one entity



The following figure shows a proposal zone model for a system railway in a standardised and modular way, including Business-IT and gateways to other entities or the internet and other RU/IMs at a high level.

Figure 7 Example of a proposal railway system zone model concerning TS50701 (Source: CLC/TS 50701:2021 - © CENELEC, reproduced with permission)



SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 4.4
EN62443-3-1	CHAPTERS 5 TO 16

3.1.5 Domain specific guidance

3.1.5.1 Signalling
A set of possible assets and requirements can be found in documents from the EULYNX project.

3.1.5.2 Rolling stock
A set of possible requirements is found in Annex G of CLC/TS 50701:2021.

3.1.5.3 Fixed installations
No deviations.

3.1.5.4 Office and business
For office and business IT, it is most likely that an inventory of assets will exist, either for accounting purposes or due to tax obligations.

3.2 INITIAL RISK ASSESSMENT (ZCR 2)
Guiding questions: What risks is my system prone to? What will I have to consider in later stages?

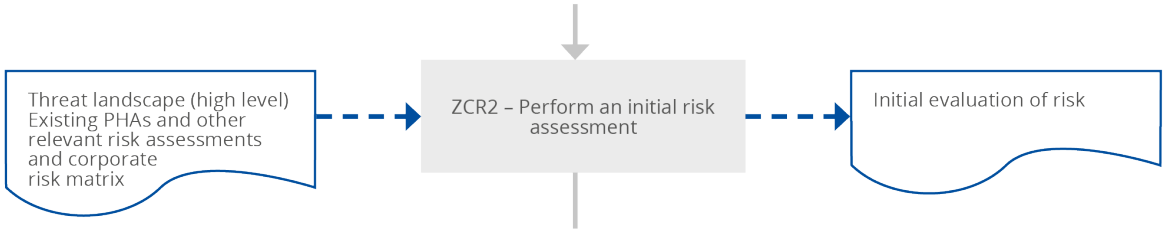
3.2.1 Process
After the assets and SuC are identified, the initial risk assessment should be performed. This process identifies and prioritises specific processes or utility areas of the SuC by their relative importance to the asset owners' business.

For the railway application, at least the following criteria should be considered:

- human health and safety
- operational availability
- financial impact.

Hint:
ZCR2 identify global and company risks.
ZCR4 identify and verify high-level risk by using the proposal zone model

Figure 8 Initial risk assessment to identify sources of high-level risk (ZCR 2)



3.2.2 Relevant parts of standards

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.3 AND 6.3.1
EN 62443-3-2:2020	CHAPTER 5.3

3.2.3 Design information

No additional information.

3.2.4 Additional guidance

3.2.4.1 Cookbook step 2: identify corporate risks

Input

- the draft of the proposal zone model and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communication scheme on a high level with conduits and boundaries, or at least a record of the boundaries and points of access to the SuC and each process.
- draft of zone critical (ZC) levels and a communication matrix (CM).

Tasks

1. Perform an initial risk assessment:
   - Identify risk scenarios and worst-case consequences for the risk events of loss of confidentiality, integrity and availability for each process or utility area and the SuC. The high-level security objectives of confidentiality, integrity and availability are commonly used within information security and are further developed into seven foundational requirements by the IEC 62443 series.

Note: The worst-case consequence is limited to a span of x calendar day(s), which must be defined in the enterprise risk management tools.

In addition, impacts that continue beyond a defined number of calendar day(s) should be considered within plans for business continuity and resilience.

- Assess the description of the consequences and rating for each area of impact (entity) using the company's risk criteria as defined in the risk management tool.

Hint: the detailed risk assessment process does not assume a fixed likelihood.

- Assess the description and rating of the risk for each identified risk.
- Determine the highest risk rating for each process or entity and the SuC.

2. Validate the draft of the high-level railway system zone model:
- Assign the highest risk rating for each process or entity and the SuC as the critical rating.
- Note: as likelihood is assumed to be fixed, this document refers to the high-level risk rating simply as the critical rating.

3. Validate the communication matrix and critical zone levels.

4. Validating all results through an impact evaluation.
The impact evaluation in the initial assessment of risk should identify the worst global impact in case of loss of the properties of an asset. The global impact should be evaluated not only at the business level, but also at the environmental, societal, and human impact levels.

Output

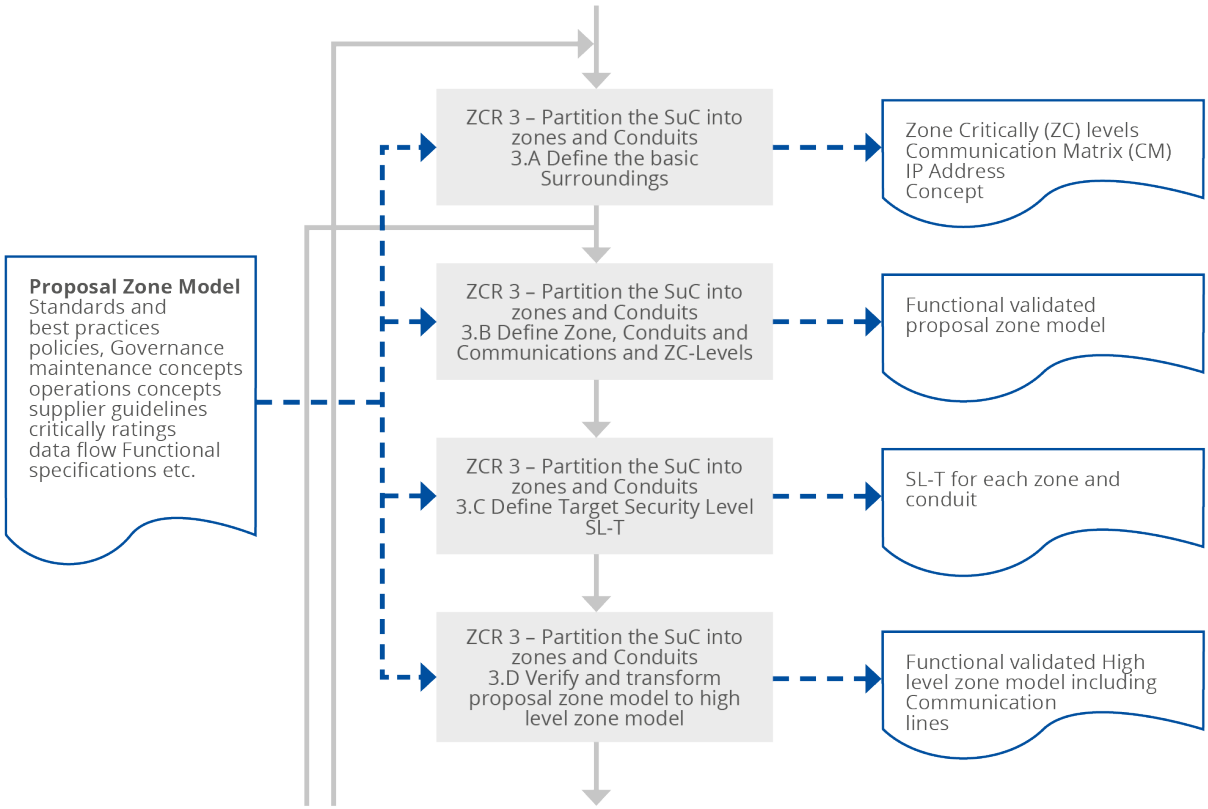
- Negative validation: go back to Step 1.A and redesign the proposal zone model
- Positive validation:
  - go forward to ZCR 3 / Step 3 'Zoning'
  - risk validated:
    - proposal zone model and high-level documentation for:
      - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC);
      - zones in the organisational SuC;
      - technical SuC such as interlocking systems or substations;
        - communication scheme on high level with conduits and boundaries;
        - records of the boundaries and points of access to the SuC and each process;
    - the documentation shall include at least:
      - high level risk matrix,
      - high level risk evaluation.

3.3 PARTITIONING OF ZONES AND CONDUITS (ZCR 3)

Guiding questions. How to do zoning? How can I divide my system using good partitions? What criteria should I use?

3.3.1 Process

Figure 9 Partitioning and SuC process (ZCR 3)



SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4
EN62443-3-2	ALL CHAPTERS

3.3.2 Relevant parts of standards

Criteria for zones and conduits breakdown

Based on the output of the initial risk assessment, the assets should be assigned to consistent security zones connected by conduits. This means all assets in the same zone and all data sent by the same conduit share the same or similar cybersecurity requirements.

The following criteria should be used to partition the SuC into zones and conduits:

a. risk to the assets in terms of integrity, availability and confidentiality;
b. type of interfaces or connections to the other parts of the SuC (e.g. wireless);
c. physical or logical location;
d. access requirements;
e. operational function;
f. organisation responsibilities for each asset;
g. safety aspects;
h. technology lifecycle, e.g. product lifecycle, obsolescence [Source: CLC/TS 50701:2021].

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4.1

Process for breaking down zones and conduits

The objective for grouping the assets into zones and conduits is to identify the assets that share common cybersecurity requirements and group them to share the means of mitigation. The following aspects should be considered for the process of defining zones and conduits.

- The business assets (IT) and control assets (OT) should be separated into different zones.
- Safety-related assets shall be grouped in dedicated zones which are logically or physically separated from zones which are not safety related. However, if non-safety assets are allocated to such a zone, the complete zone is considered as safety related.
- Temporarily connected devices should be included in zones separated from assets that are permanently connected.
- Wireless devices should be included in zones separated from the ones with the wired devices.
- (Remote) Devices that are permitted to make connections should be grouped into a separate zone(s).
- Zones should contain the security device protecting the perimeter at the edges of conduits.

Attention: exceptions from the above requirements should be verified by risk analysis. [Source: CLC/TS 50701:2021]

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4.2
EN 62443-3-2	CHAPTER ZCR 3-2 TO 3.6
EN 62443-3-3	CHAPTER SR5.2

3.3.3 Design information

3.3.3.1 Remote maintenance access

a) **With** a possible impact on system operations

The following design rules should be considered for maintenance application:

- direct (maintenance) access from business zones or from external sources to OT zones with higher security demands, e.g. up from ZC4 (depending on the individual ZC Model) or SL2 without control by an internal security device or similar (e.g. proxy server), should not be allowed;
- external maintenance access (e.g. via Internet) should be grouped, controlled and forewarned in a separate internal zone, e.g. maintenance access via a B2B proxy in the technical DMZ.

b) **Without** a possible impact on system operations

The following design rules should be considered for devices communicating with mobile phone networks so that misconfiguration or sent commands don't have any impact on normal operations, e.g. datalogger, sensor values by IoT devices:

- direct (maintenance) access from business zones or external to control zones without control by an internal security device or similar (e.g. proxy server) is allowed if the source (sensor, device, IoT-edge) and the sink (collecting server) are in special and separated zones;
- it is highly recommended, in order to guarantee the integrity of data, to encrypt communications via unsecure or untrusted networks.

3.3.4 Additional guidance

3.3.4.1 Cookbook step 3a: defining global surroundings

Before starting to plan zones, basic information on the company and its surroundings needs to be defined. These basics concern the environment, devices, systems, employees etc. and may differ for each company.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX F.2.2 (LANDSIDE)
CLC/TS 50701:2021	ANNEX F.2.3 AND F2.4 (ROLLING STOCK AND OVERLAPPING)

Task: Define 'classes of networks' by the maturity of their security

Firstly a set of 'network classes' needs to be defined. Each network class will have a unique security maturity. This is needed to generate a communication matrix to determine which dataflows are allowed or not allowed.

Too many network classes increases the ruleset, make the overall concept complex and obstruct upcoming functions which merge data of different sources to support AI, Digital-Twin, and Condition based Maintenance. On the other hand too few network classes reduce security and resilience. Figure 6 shows an example of a set of networks for one entity.

Hint: an odd number of network classes and placing the internal network in the middle is 'neutral' with 'medium security maturity' and is recommended.

3.3.4.2 Zone criticality (ZC)

Every zone should be classified according to its risks. Zone criticality represents the security demands in a simplified expression to define the allowed communication between zones. Zone criticalities represent the individual network groups based on the maturity of their security and should cover all zones in the owner's company.

Note: *to take care of the different system architectures in Rolling Stock Systems and Landside, two schemes of Zone criticality are available:*

- *Zone criticality landside (ZC-L),*
- *Zone criticality rolling stock (ZC-RS). [Source: CLC/TS 50701:2021: F2.3.x and F2.4.x]*

An example can be found in CLC/TS 50701:2021 Annex F.4.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX F.4

An example of possible zone criticality levels can be found in CLC/TS 50701:2021 Annex F.6.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX F.6

3.3.4.3 Communication matrix (CM)

The communication matrix defines, at a high-level, authorised and unauthorised communications. The matrix is unique within a company and valid for all communications and entities in one company (RU or IM). The communication matrix is the basis of rulesets for security devices to control dataflows between zones to prevent loops, backdoors or the bypassing of security measures and is based on levels of 'zone criticality' (ZC).

Referring to a castle: the communication matrix is the code of contact on which all inhabitants agree; it defines who can go to which areas in the castle. Is it allowed to read or write books in the archive? Who can pass the kings security to enter the princess bedroom?

Note: the definition of which book is read only or enabled to write is the result of the ruleset for security devices.

A communication matrix will be developed based on the following two rules:

- direct communication between zones with well-known risks (e.g. zones with well-known and fixed mounted OT devices) and unknown risks (e.g. office zones with laptops, printer, internet connectivity) should be refused;
- in general, direct communication is only allowed between zones with the same or a subsequent zone criticality.

3.3.4.4 Communication matrix (CM) and zone criticality (ZC)

The communication matrix shows, at a high level, which communications between zones are allowed, restricted or prohibited. This matrix is one of the basics of the final zoning model. It is also a helpful, simple and easy to understand overview for technicians in their daily business if systems expand or new functions need to be implemented.

Attention: the final CM and the ZC principles need to be part of the internal ISMS. This is the basis for all (future) communication flows, systems extensions, new features and firewall rulesets.

The dataflows should be defended and controlled based on the safety and security demands of the zones. The fine tuning of dataflows is controlled by rules and access lists (e.g. of the security devices):

- "+" data flow is allowed in both directions,
- "R": data flow is restricted to read-only only by data diodes or similar measures,
- "-": data flow is prohibited.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX F.5
CLC/TS 50701:2021	ANNEX F.7

3.3.4.5 Cookbook step 3b: define zone, conduits, communication lines and ZC-levels

Input

- Approved CM and ZC principles.
- Risk validated
  - proposal zone model and high-level documentation of:
    - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC);
    - zones in the organisational SuC;
    - technical SuC such as interlocking systems or substations;
    - communication scheme on high level with conduits and boundaries;
  - records of the boundaries and points of access to the SuC and each process.

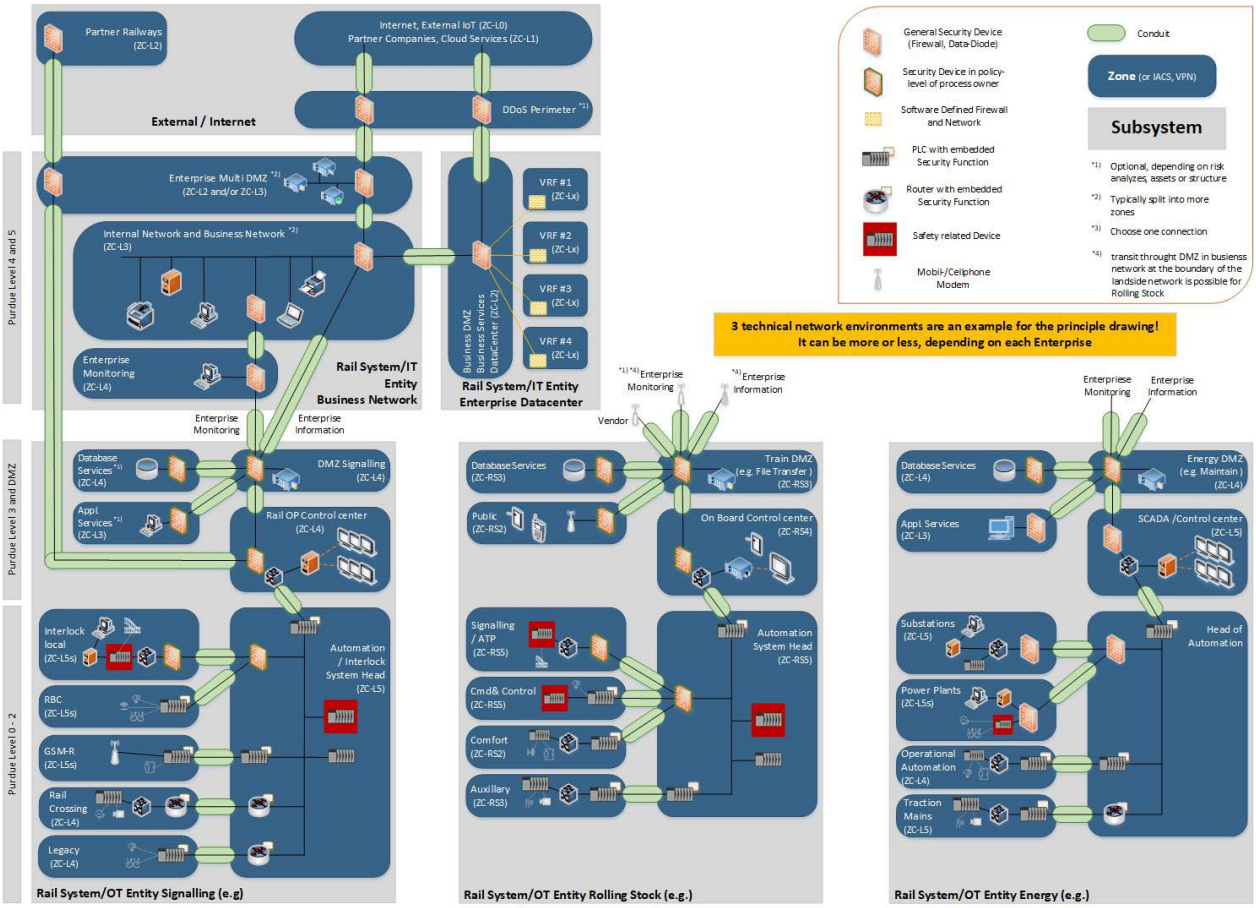
Task: Defining zones in the proposal zoning model

Hint: the following chapter can be used as a checklist.

1) Take all asset groups identified in ZCR 1 and verified in ZCR 2 and try to define a zone model based on the system and device communications. The high-level railway zone model can be used as layout for the first attempt.

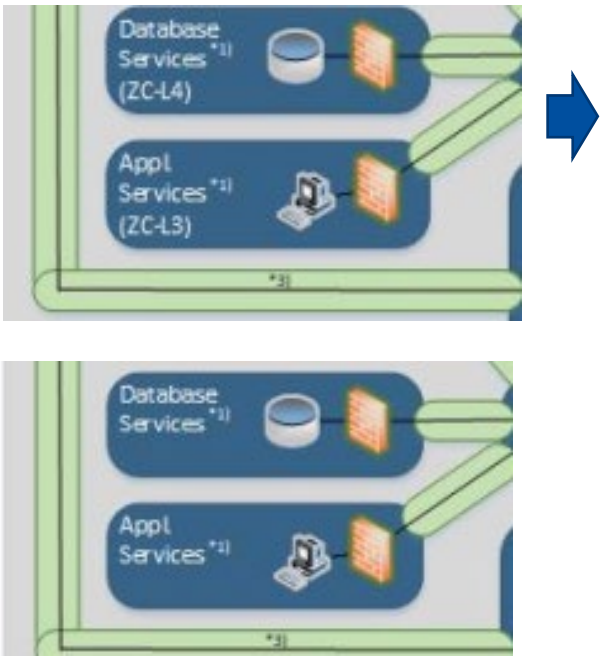
2) Extend the generic high-level zone model to a company specific model with all organisational or technical SuCs and zones.

Figure 10 Example of an individual railway zone model



3) Classify each zone with a zone criticality (defined in the CM).

Figure 11 Example of defining zone criticality in the individual railway zone model



4) Conduits: place security devices on the boundaries of each zone.

5) Check normal dataflow between zones and their ZC with the validated CM if the process communication of the essential functions is working well.

6) Check the dataflow for system diagnostics between the zones and their ZC with the validated CM if the process communication of the essential functions is working well.

Figure 12 Example 1 of possible communication flow

ZC-L 4	secure	data centre, internal DMZ, ICS/automation	-	+	+	+	-	-	-
ZC-L 3	medium	internal network, office and business network	-	-	+	+	+	+	-
ZC-L 2	low	gateway area, external DMZ	-	-	-	+	+	-	+

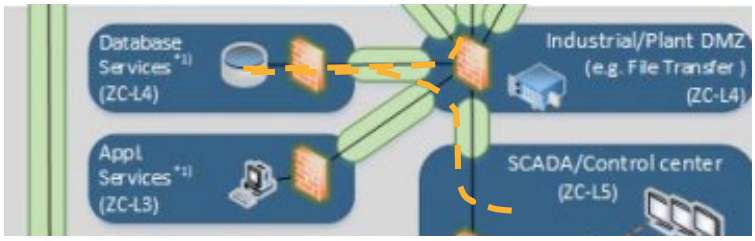
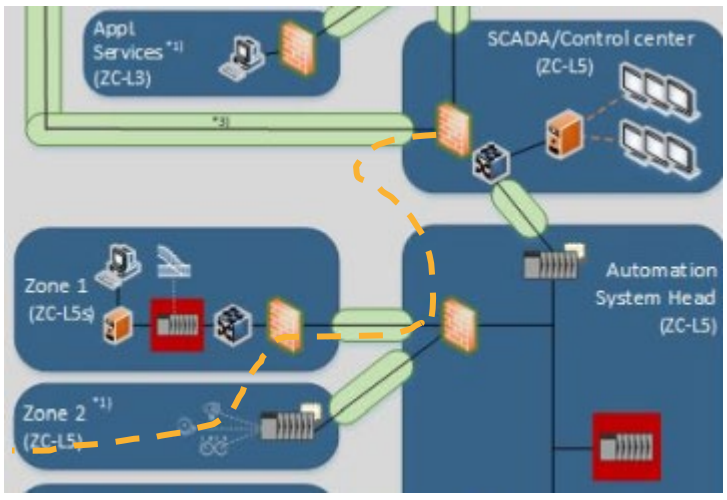


Figure 13 Example 2 of possible communication flow



7) Place means for monitoring management systems (technical domain controller, network management, NAC, PKI, Syslog & SIEM, etc.) in every organisational SuC to support the 'de-centralised approach' and the 'modular entity subsystem approach'.

Note: in some cases, functions may not be working. This results in a step back to ZCR 1 or ZCR 3a (depending on the severity of the challenge) and the redesign or relocation of the zone or document (and finally approved) expectations.

8) Check if the communication flow will work with the relevant devices. It is possible to merge and/or reduce zones in a second loop if approved by a risk analysis.

9) Check the methods and strategies for patching and updating to all zones and all devices

10) Check communications with partner companies, other IM and RU or Cloud connectivity.

11) Check corporate goals and strategies (can be read from the ISMS).

12) Check remote maintenance connection (personal support and configuration of data transfer) and close all existing connections bypassing the official way and authorised methods (modem or ISDN, for example).

13) Check authentication, user rights and role mechanisms. Is it possible for each single device to check the authorisation if a user wants to log in?

14) Check whether the dispatching and operating staff have the awareness to understand the overall concept and to handle the security mechanisms in the correct way in order to prevent unknown backdoors.

15) Check whether the dispatching units have sufficient knowledge about functional processes and the security organisation.

16) Check whether the zoning architecture forces the same security requirements for backup LAN/WAN connections.

17) Check whether the zoning architecture includes zones for system backups and individual P-V-LAN's. Otherwise, the 'normal' network must be separated into different zones to increase resilience, but all backup connections will target into one backup zone, bypassing the segmentation.

18) Check all zoning relevant controls of ISO27001 that are not listed above.

19) Start merging de-centralised managing and monitoring systems at point 6 if that is possible. After each merge, check the CM requirements and the administrative requirements.

20) Note all results and expectations for a zoning design report
The following items should be identified and documented for each defined zone and conduit:
    a. name and/or unique identifier also indicating the type (zone or conduit);
    b. accountable organisation(s);
    c. definition of logical boundary;
    d. definition of physical boundary, if applicable;
    e. safety designation;
    f. list of all logical access points;
    g. list of all physical access points, if applicable;
    h. list of dataflows associated with each access point;
    i. connected zones or conduits;
    j. list of assets and their risk classification and business value.

21) Check restrictions on (external) maintenance access in the '(Remote) Maintenance access' chapter.

22) Take all asset groups identified in ZCR 1 and verified in ZCR 2 and try to define a zone model based on the system and device communications. The high-level railway zone model can be used as a layout for the first attempt.

23) Extend the generic railway model to a company model with all organisational or technical SuC and zones.

Hint: this zoning step takes more than one iteration until it is finalized. Take care about this!

Hint: It is recommending defining a set of security functions and parameters for each group of assets. This helps the technicians and the vendors to implement and use the correct function and settings. Details see Annex D

Hint: with background knowledge about the essential functions, it is possible to hasten the process instead of following the next steps and come back from ZCR 4 or ZCR 5 (risk assessment).

Task: Defining conduits in the proposal zoning model

Conduits represent a zone's gateway or interface enabling it to communicate with other zones. In general, there are three kinds of zones and each results in a different conduit solution.

- A zone containing a lot of local devices: these OT devices share the security device on their zone's conduit. From the economic view, to buy, manage and operate a high-level security device is relatively cheap.

- A zone consists of one (or very few) devices. It called a 'single system area' (e.g. PLC for lightning board in small stations). To secure this device, three options are possible:
  (a) Professional security device from network provider in each control enclosure … very expensive
  (b) Industrial security device in each control enclosure … expensive
  (c) Embedded security in the ICS/PLC … cheap to buy and operate.

Example PLC:

  - If the device doesn't fulfil the security requirements, it is necessary to add a mitigating measure such as an industrial firewall in front of the device to minimise the residual risk.
  - If the device has a set of embedded security functions (e.g. SNMPv3, AD and RADIUS, VPN and PSK, Syslog) and fulfils the requirements, no additional measures are needed.

- A zone contains safety devices. In this case, the security device must fulfil the specific demands for safety, e.g. 'read only' devices like data diodes of network TAPs or a special configured firewall with certifications.

Task: Systems without full security functions (legacy, PLC etc.)

All traffic within a security zone is likely trusted (on a practical note: not all industrial devices can handle the necessary level of cybersecurity). The cybersecurity checks are executed on the border of the security zones (within the conduit).

Hint: the chosen 'proposal' for each conduit IN THIS STEP depends on the amount and security capability of the devices.

Note: conduits don't need a ZC-Level. Conduits act as perimeter protection for the zone 'behind' and must fulfil the **security level** of and for the Zone.

Task: Defining communication lines in the proposal zoning model

Local communication lines are necessary to enable process communication. These lines are mostly located in a defined or small area, building etc. Normally it is not possible to connect without special tools, keys and knowledge about the location but it is not necessary to encrypt, e.g. connecting devices within a closed control enclosure.

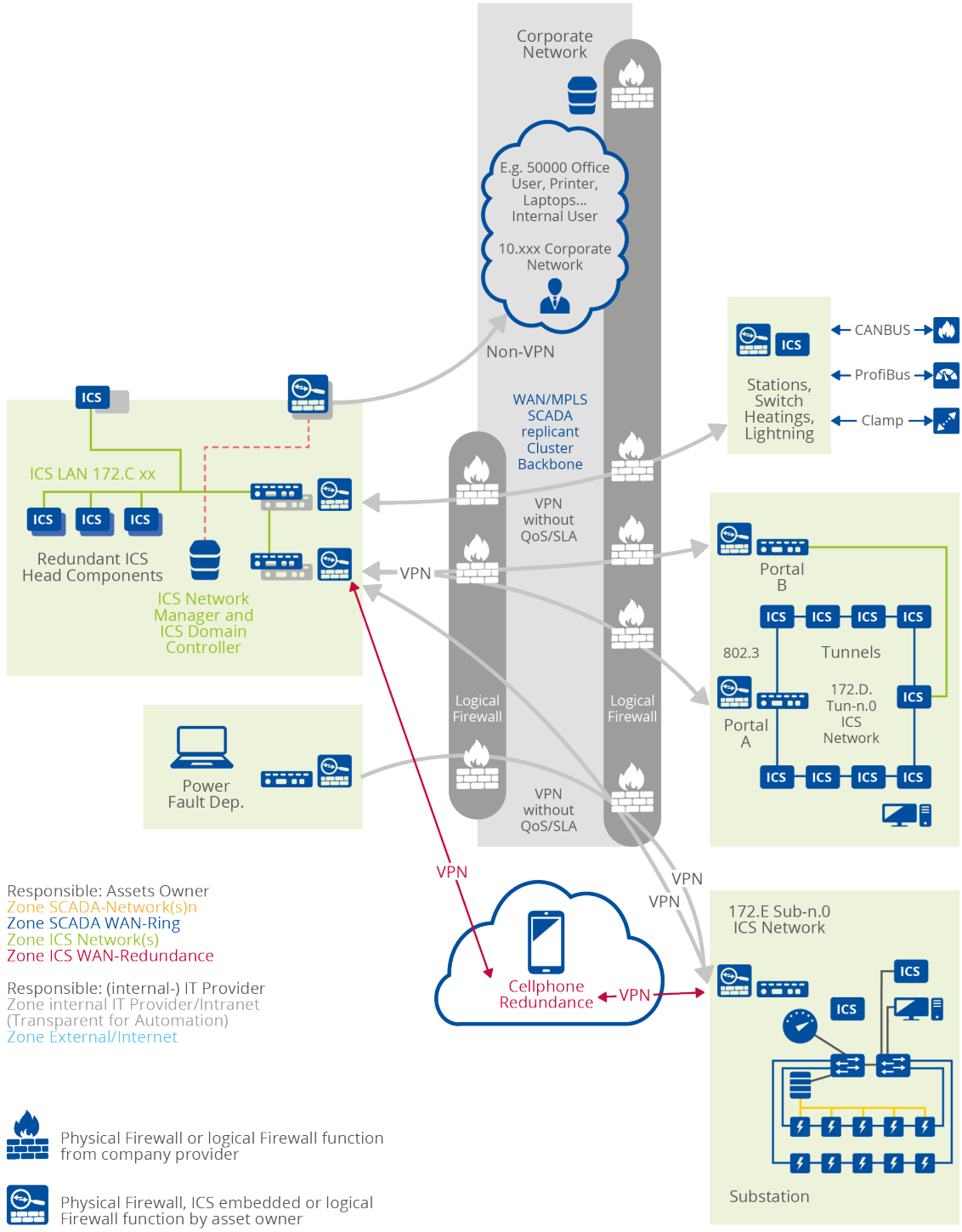
Note: measures on local communication lines must be documented and aligned with the CISO.

WAN Communication lines can be seen as 'transparent' for ZC if the security gateways on both sides of the 'tunnel' are managed by the responsible asset owner or owner of the essential functions.

'Transparent' means:

- there is no possible impact on the dataflow by the provider (e.g. VPN);
- it is theoretically possible to change the provider **without** any changes (except WAN IP Address to VPN) or **without testing all systems and essential functions** behind the security devices.

Figure 14 Example of transparent communication lines between zones



Note: the security gateways must fulfil, on both sides, the same SL and the communication must be encrypted for SL1 or higher.

Hint: it is recommended that the tasks from 'defining zones in the proposal zoning model' to 'systems without full security functions (legacy, PLC etc.)' be repeated for an extra iteration to review all topics before going forward.

IP address concept

- Input factors
  - Every device interface needs a unique (company net) or NAT (entity net) IP address.
  - Every device with redundant communication (VRRP/HSRP) needs a unique loopback address.
  - Every VLAN needs a unique (company net) or NAT (entity net) IP address range.
  - Every zone needs a unique (company net) or NAT (entity net) IP address segment.
  - Every secure communication line (VPN) needs unique (company net) or NAT (entity net) IP addresses.
  - Sometimes the IP addresses are existing and easy to readdress. Some systems have a historical background (Token-Ring) or are in 7/24 operations and readdressing generates a lot of cost.

- Task (IP address ranges may be an example):
  Creating an IP address concept based on one of the two general principles:
  a) Segmented but flat IP network with central firewall
     Example: all IT and OT devices in 10.x.x.x.

  b) Mixed hierarchical NAT network with decentralised firewalls (Defines in depth principle)
     Example: IT devices and OT entity forwarding addresses in flat 10.x.x.x, OT devices in 172.16-32.x.x, backup and local field sub-devices 192.168.x.x.

- Challenge
  To avoid IP address conflicts, especially in the overall railway system, an IP address concept is one of the most important things to do.

Hint: a NAT concept for each SuC or entity with a couple of reachable forwarding addresses from the intranet, makes the concept more flexible, faster, easier and increases the availability in cases of changes. Otherwise, one change in one entity causes a globally redesign over many Systems within the company!

Hint: a VPN between zones normally acts company wide. It is highly recommended that one global additional IP Segment for VPN addresses be reserved!

Hint: to manage devices with redundant connections in case of losing one connection, its recommended to address the device for management tasks or network management by a separate logical loopback address which is virtual connected on both interfaces

Hint: Its highly recommended to reserve one additional IP Segment in every entity for HSRP/VRRP or loopback addresses!

Note: Every change of an IP address causes an interrupt of data and communication. To be on the safe side, the devices outside the central system shall be configure and restarted local. Readdressing a whole segment means, to build up a secondary virtual interface to migrate one by one. Keep in mind and plan ONE future-oriented IP address concept.

Output

- functionally validated proposal zone model and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communications scheme on a high level with conduits and boundaries,
  - IP address concept (zones and transport net);
- functionally validated zone criticality (ZC) levels and a communication matrix (CM);
- a zoning design report.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX F.2.2.2
EN62443-3-1;20XX	CHAPTER 5-16
EN62443-3-3:20XX	ALL CHAPTERS

Note: at the end, an approval of the CISO or ISO is necessary. It is highly recommended that the following steps be undertaken as a group made up of the asset owner or owner of the essential function (= ISE) the ISA and ISO/CISO.

3.3.4.6 Cookbook step 3.c: define proposals for target security level (SL-T)

After partitioning and zoning the SuC, the threat agents should be identified and an initial minimum-security level target (SL-T) should be assigned to each security zone within the SuC and the entity.

Note: 'Zone' is a group of assets. 'SL' is a definition about the power of the perimeter security to protect the group of assets. So, the SL must apply to the security device on the zone conduit.

Input:

- functionally validated proposal zone model and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communication scheme on a high level with conduits and boundaries;
- zones with functionally validated zones criticality (ZC) levels and a communication matrix (CM);
- a zoning design report.

Task

The steps for assigning the initial SL-T are as follows:

1. Determine whether specific threats that intend to target the SuC, zone or similar IACS, automation solutions and products, exist longer than the design lifecycle of the SuC.

Hint: if no specific threats exist then categorise general threats as either 'internal' or 'external'.

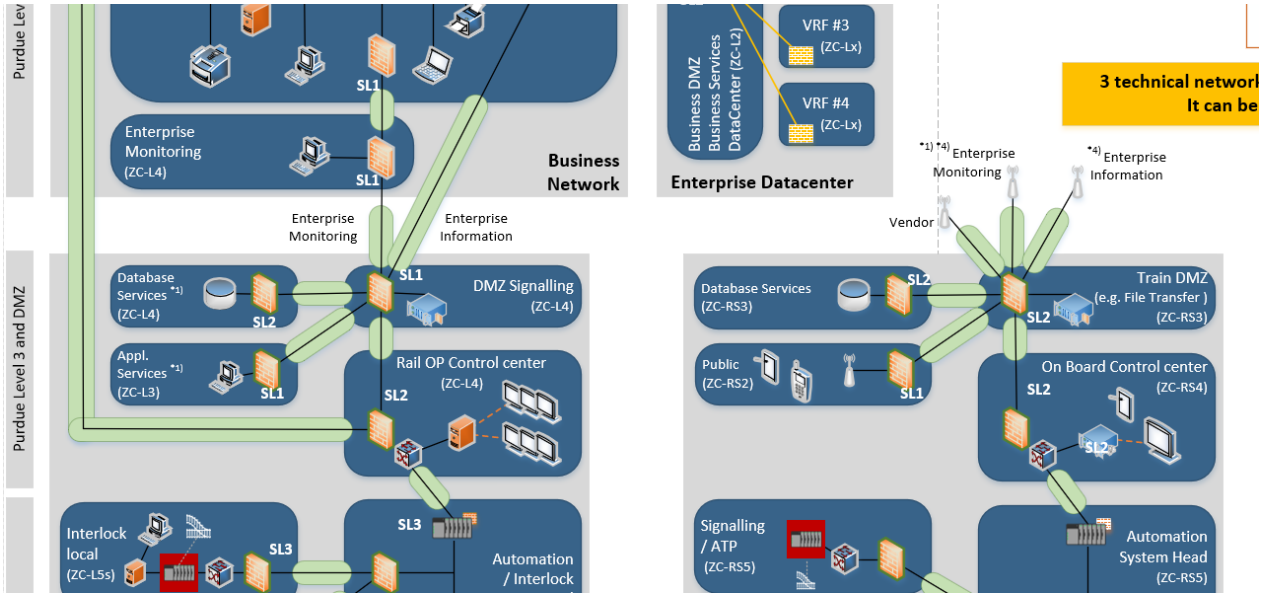
In conventional security risk management, a threat is a function of intent and capability. With respect to cyber risk management, the threat environment is continually and rapidly changing to the point where the attribution or characterisation of threat agents to a specific entity is of limited benefit.

2. Evaluate the intention, resources, skills and motivations of threat actors and the possibility attacks over the design life of the SuC.

3. Assign a minimum-security level target (SL-T) to each security zone. Every conduit on a zone or SuC should be mapped to an SL between 0 to 4 which defines the strength of the resistance against hacker attacks.

Note: system costs increase proportionally with the mapped SL.

Figure 15 Example of defining SL to each zone and conduit



4. Depending on the location in the company model, this results in a strengthening of the encryption and security features of the security gateways between each zone and conduit.

Note: the chosen SL depends on the security needs of the overall railway system. A higher SL may cause problems in process communications and may require the development of special solutions. This must be clarified with the system vendor.

5. Check whether the chosen SL-T allows the process communication relationships of the OT systems to operate.
   Example:
   - Now: the communication between two devices is hardcoded by the system and has been running for 10 years.
   - Plan: separate the devices into two different zones with SL2 at one conduit. SL2 means multifactor authentication is needed.
     - Problem: how to integrate an automatic MFA via SMS e.g. in a 10 year old application?

6. Check if the security devices on the conduits support measures needed to force the SL-T. If not, replace the device to fulfil the demands of the SL. The feedback is an input for the risk assessment that follows in ZCR4.

Output:

- definitions of SL-T for each conduit or zone and the minimum-security strength for the gateway devices on the conduit;
- list of minimum functions for the functional requirements (FR) and system requirements (SR);
- security vector based on measures for FR and SR;
- records of threat agents;
- records of minimum SL-T for each security zone.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 8
IEC 62443-1-1	CHAPTER 8 (FR)
IEC 62443-3-3:2013	ALL CHAPTERS, ANNEX A

3.3.5 Domain specific guidance

3.3.5.1 Signalling

Currently the proposed SL-T for devices in the signalling domain is SL-T 3. In some cases, SL-T 2 is also applied, which depends on the risk for the zone. Details can be found in the EULYNX baselines.

3.3.5.2 Rolling stock

A set of possible requirements is found in Annex G of TS50701:2021.

3.3.5.3 Fixed installations

Attention: **for fixed installations, all zones must fulfil the requirements for SL1 at least!**

For multiple and redundant real-time communications, make sure that all conduits are related to this zoning model, and check that the run time delay of all communication channels and conduits do not differ too much, lest the redundant heads of automation control systems starting master/slave switching.

Redundant automation or SCADA systems are designed to send out redundant IP packets and need redundant acknowledgements. Standard firewalls recognised the as DDoS or Syn-Flood attacks and turn off communication or throw away the excessive acknowledgements.

A set of recommended requirements is provided in an additional and following paper “Common Security Baseline”.

3.3.5.4 Office and business

No deviations.

3.3.6 Design information

3.3.6.1 Step 3.D: the architecture review or from the proposal to the ‘high-level zone model’

This step seems like step 3.2 before, but more details are available. It is a second deep-dive iteration for verification and validation.

Input

- ZCR 1: proposal zone model with asset groups;
- high-level documentation of:
  - organisational SuC (or ‘subsystem’ to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communication scheme at a high level with conduits and boundaries,
  - asset and asset groups;
- ZCR 3a: surroundings: validated zones criticality (ZC) levels and a communication matrix (CM);
- ZCR 3b: proposal zone model with defined conduits and process communications;
- ZCR 3c: proposal for the security levels for each conduit (zone and SuC);
- SL-T defined for each zone.

Task: Verify it

Take the proposal zone model (output from chapter ‘ZCR 3c’) and perform a crosscheck on all

> Hint: the following chapter can be used as a check list.

needs up to this point.

1) Take the proposal zone model with the asset groups (‘zones’) from ZCR 1b.
2) Check the ZL and CM from ZCR 3a, because they are valid for the whole company and are not changeable.
3) Check the communication flow against:
   a. process needs;
   b. IP address concept and gateways for
      i. Data and Information (“message direction”)
      ii. Service access to maintain devices (“command direction”);
   c. principles from chapter ARCHITECTURE AND DESIGN PRINCIPLES;
   d. principles from chapter SYSTEM PRINCIPLES.
4) Check zones, conduits and security gateways in the proposal zone model (ZCR 3b).
5) Check security levels (ZCR 3c).
6) Check the communication flow against:
   a. process needs;
   b. vendor specific configuration on the B2B proxy in the technical DMZ for remote maintenance and storage of ICS configuration data;

c. principles from chapter ARCHITECTURE AND DESIGN PRINCIPLES;
d. principles from chapter SYSTEM PRINCIPLES.

Hint: this step of zoning takes more than one iteration until finalised. Take care with it.

If all communications and systems work (approval by asset owner), the boundaries and the security devices, the IP addresses and other topics seem manageable then you have passed the first big milestone.

Output

- Validated high level zone model and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC);
  - zones in the organisational SuC;
  - technical SuC such as interlocking systems or substations;
  - communication scheme at a high level with conduits and boundaries;
  - IP address segments for planning to provide and configure the network devices before starting migration;
  - location and type of security devices;
  - list of Back2Back proxies in the technical DMZ for terminating the communication;
  - list of systems and services that need to migrate from old to new zones as a basis for passing money, human resources for changes and planned project milestones;
  - list of Layer 3 Segments, Layer 2 VLANs and IPsec/TLS Tunnels;
  - security vectors for FR und SR for every conduit (zone and SuC).
- Functionally validated zone criticality (ZC) levels and a communication matrix (CM).
- A zoning design report.

3.4 HIGH LEVEL RISK ASSESSMENT (ZCR 4)

Guiding question. What impact could an attacker have on my system?

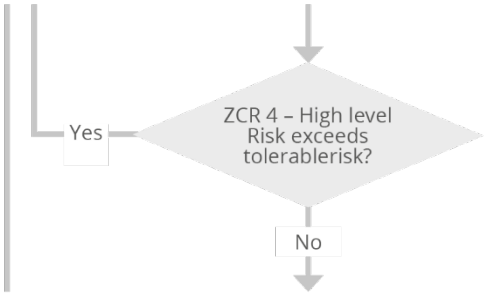
3.4.1 Process

For each asset group supporting the essential functions of the SuC, the consequences of losing the integrity, availability or confidentiality of the asset should be evaluated.

To enable a consistent approach for threat risk assessment between asset owners, system integrator and product suppliers, it is important that all the stakeholders share the same references for impact assessment.

Note: the decision steps of ZCR 4 High-level Risk Assessment differ between railway system needs and the generic standards in 62443-3-2.

Figure 16 High-level risk assessment process (ZCR 4)



SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4

3.4.2 Relevant parts of standards

Likelihood assessment

'The threat landscape may change suddenly and so experience is of limited use for cybersecurity. Therefore, the likelihood of an attack can be evaluated only on a qualitative or semi-quantitative scale. Because of that, the owner of the essential functions should make use of intelligence reports and other information sources to determine the potential attackers that they might be targeted by.' [Source: CLC/TS 50701:2021]

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.2.5

Threat assessment

To build an appropriate cybersecurity strategy, shared between all the stakeholders, the first step is to identify and agree on a consistent list of generic cybersecurity threats that could jeopardise the railway application. Agreement on the threat landscape is crucial as discrepancies in the set of threats considered by the different stakeholders will lead to an underestimation of risk and a lack of implementation of control measures.

Threat libraries and reports such as the following should be taken as inputs:

- ENISA Threat Landscape Annual report,
- ISO/IEC 27005,
- NIST SP 800-30.

Finally, the threat landscape should:

- be defined or at least approved by the asset owner;
- be updated at least once a year (or according to contractual requirements);
- provide mapping to the input threat libraries or reports;
- provide rationale for threats excluded from consideration [Source: CLC/TS 50701:2021].

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.2.6

The cybersecurity requirements specification (CRS)

A cybersecurity requirements specification (CRS) is established for each zone, SuC and conduit. It shall be reviewed against general cybersecurity requirements based on company specific policies, standards and relevant regulations and shall be approved by the railway asset owner and duty holder.

As a minimum, the CRS shall include or refer to the following:

- list of detailed security requirements, including SL-T, assumptions and security-related application conditions;
- SuC description;
- zone or conduit drawings;
- zone or conduit characteristics;
- operating environment assumptions;
- threat environment;
- risk acceptance;
- regulatory requirements [Source: CLC/TS 50701:2021].

3.4.3 Design information

No additional information.

3.4.4 Additional guidance

3.4.4.1 Cookbook step 4: high level risk assessment - verifying high-level zone model against cyber risks

A specification of cybersecurity requirements must be drawn up in accordance with CLC/TS 50701:2021.

Hint: ZCR 2 identifies global risk. ZCR 4 verifies it (exceeding or not) after putting it into zones with countermeasures

Input

- Functionally validated railway system zone model and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communication scheme on a high level with conduits and boundaries;
- Functionally validated zone criticality (ZC) levels and a communication matrix (CM);
- A zoning design report.

Tasks:

1) collect actual treat landscapes;
2) fit threat landscape to the SuC or systems to challenge against possible incident scenarios;
3) do risk assessments against all SuC, IACS or subsystems concerning how well they fit treat landscapes;

4) perform and check the input document within an assessment of likelihood;
5) perform and check the input document within a threat assessment.

Output

- Negative validation: back to ZCR 3 and redesign the railway system zone model, check the ZC and CM
- Positive validation:
  - a cybersecurity risk validated 'final zone model';
  - a cybersecurity risk validated zoning design report or document;
  - Ready to enter Level 5.

3.5 DETAILED RISK ASSESSMENT (ZCR 5)

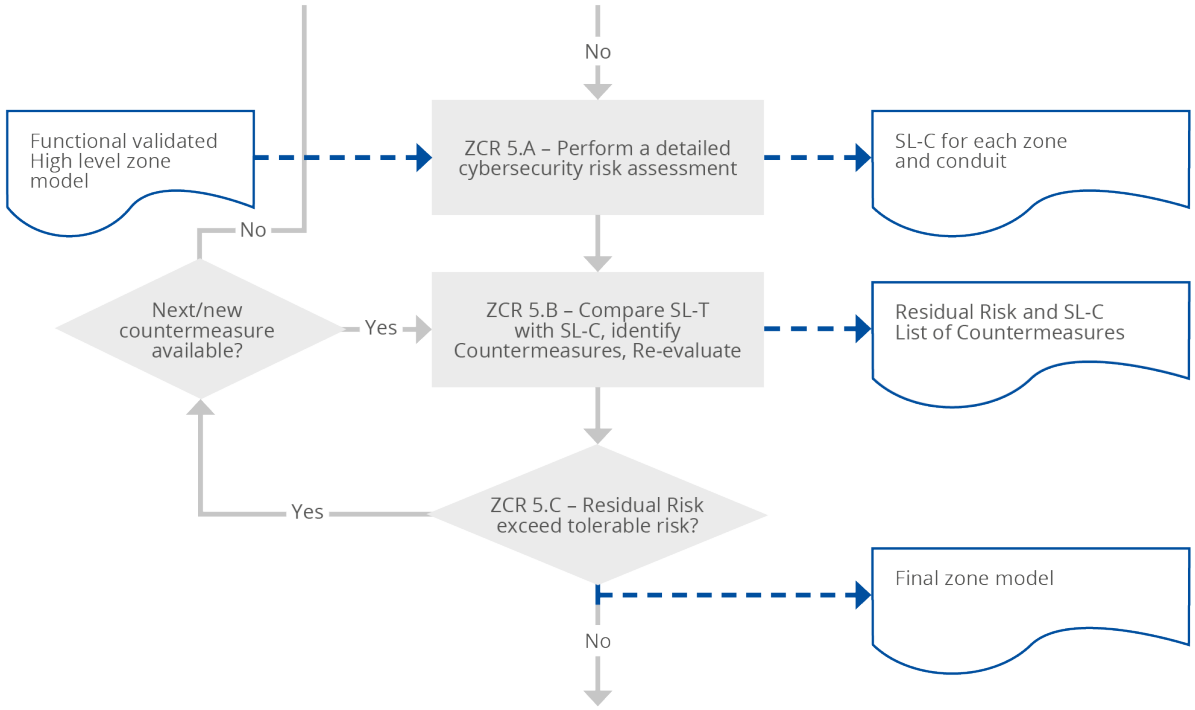
Guiding question. What security requirements are needed in order to reach an acceptable level of risk?

3.5.1 Process

The following paragraphs describe the detailed assessment of risk which should be performed for each zone and each conduit (or cluster of zones and conduits) and result in a definition of the required cybersecurity specifications as the central outcome of these activities.

To fulfil the demands of railway environments, ZCR 5 is split into three sub-processes and a step-back to redraw zones and conduits in ZCR 3 is included in this model.

Figure 17 Detailed high-level risk assessment process (ZCR 5)



3.5.2 Relevant parts of standards

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 8

3.5.3 Design information

In IEC 62443-3-2 ZCR 5.6, different approaches for the derivation of SL-T are described. The first is based directly on the need for protection against a particular kind of attacker (e.g. hacker, criminal organisation, states sponsored group), including an estimation of the efforts needed by an attacker, also known as an attack vector. This approach determines which types of attacks, by which kinds of attackers, a zone or conduit of the SuC should withstand, considering the threats and vulnerabilities identified and any legal constraints, resulting directly in a SL-T. But, in this approach, is it still necessary to check that the risk is acceptable.

Threat risk assessment may not override mandatory requirements for security protection, for example, by regulation.

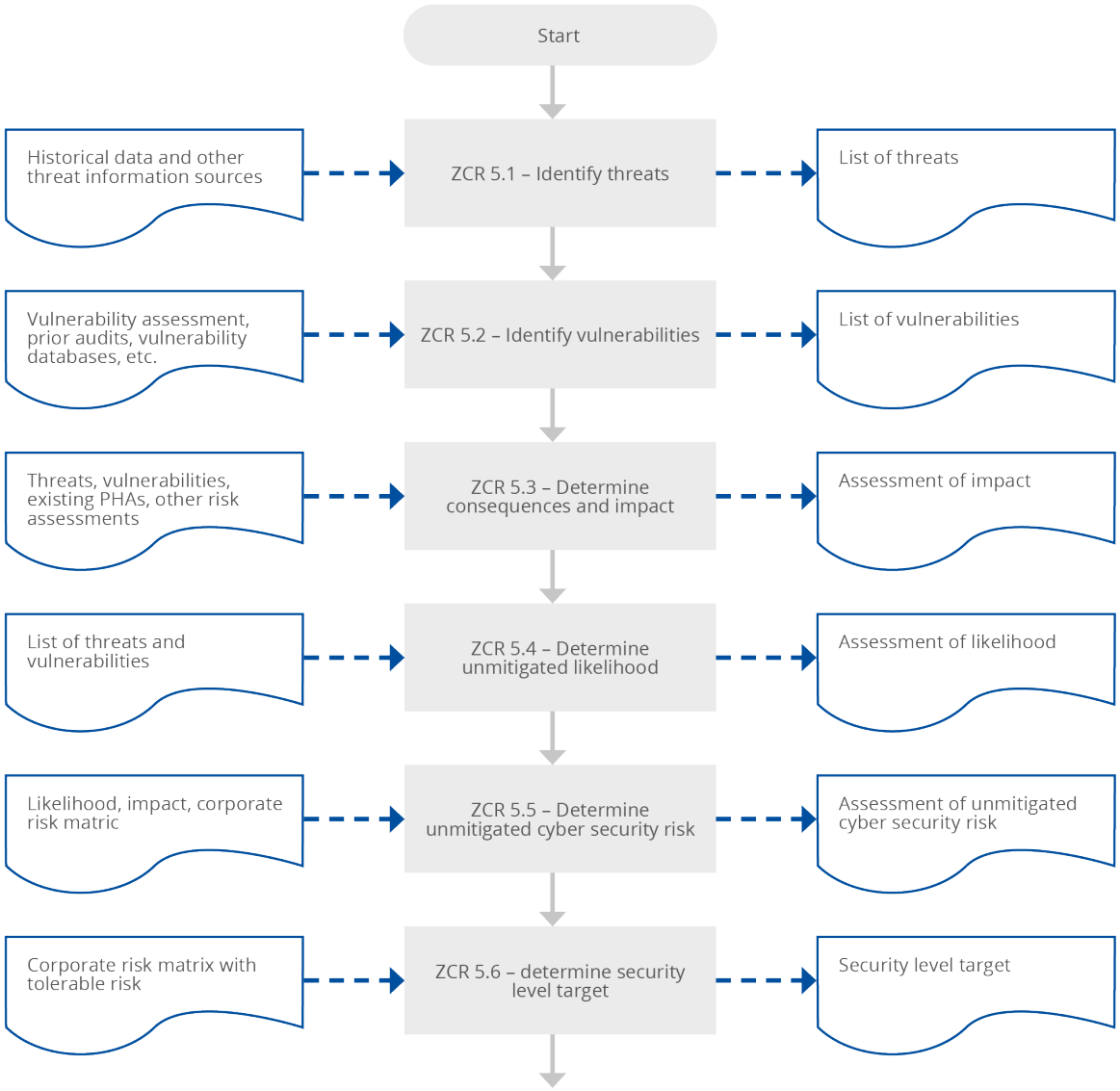
SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4

3.5.4 Additional Guidance

3.5.4.1 Process step 5a: detailed cybersecurity risk assessment

A flowchart of the general process for the detailed assessment of risk by the responsible asset owner or by the system integrator under contractual agreements, is depicted in figure 18.

Figure 18 Detailed risk assessment steps



SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 7
EN 62443-3-2	ALL CHAPTERS

3.5.4.2 Cookbook step 5a: detailed cybersecurity risk assessment

The basis of the process is the output from the high-level risk assessment (ZCR 4).

The first approach in this chapter describes the detailed assessment of risk, which should be performed for each zone and each conduit (or cluster of zones and conduits) and result in a definition of the required cybersecurity specifications, as the central outcome of this activity.

Input

- list with published security incidents, threats, and vulnerabilities
- list of the likelihoods (depending on entity and company) of incidents, threats and vulnerabilities;
- records of criticality ratings for each process or utility area and the SuC;
- records of threats;
- security advisories from product suppliers;
- historical data of security events.

In a first step, the identification of the threats and vulnerabilities are detailed. Then for all identified threats an appropriate principle of risk acceptance is chosen and approved by the railway duty holder. It is acknowledged that the easiest way to apply the process is, if only one principle is applied for each zone or conduit, for a complete zone or conduit to be covered by a code of practice or by a reference system or by an explicit evaluation of risk. But for complex systems a mixture of principles may be necessary.

Task: identifying threats in a brief

- Record all assets within each process or entity within the SuC in an asset register.
- Record all physically accessible data communications and interfaces of assets as attributes in the asset register.
- Prior to final design, obtain an independent professional review of credible threats using competent persons, who have an appropriate degree of independence.
- Keep records about the credible threats, including threat agents and threat actions, over the design life of the SuC.
- Describe the threat actions of a threat agent in accordance with the domains of attack and mechanisms of attack.
- Develop fault trees or attack trees to model the threat actions used by threat actors for each of the following general security events within the context of the SuC.

Task: The following topics shall be within the scope

- loss of confidentiality – disclosure of information assets
- loss of integrity – unauthorised use of IACS functions
- loss of integrity – modifications to IACS or information assets
- loss of availability – disruption to IACS functions
- loss of availability – destruction of IACS or information assets

After identifying the threats, the vulnerabilities in assets and countermeasures must be identified.

Task: identifying vulnerabilities in a brief

- Prior to final design, obtain an independent professional review of credible vulnerabilities.
- List the credible vulnerabilities.
- Revise the fault or attack trees to indicate credible vulnerabilities in the branches.

Task: determining unmitigated cyber risk in a brief

- Record the risks corresponding to the branches from the fault or attack tree in a risk report.

- Estimate the credible worst-case consequences and likely descriptions in accordance with the enterprise risk management tool for each risk prior to assessing the application or effectiveness of existing cybersecurity countermeasures that are not enabled by default.
- Limit the worst-case consequence to a span of x calendar day(s).
- Determine the unmitigated cyber risk rating for each risk in accordance with the enterprise risk management system.
- Record the unmitigated cyber risk in the risk report.

Task: determining security level targets in a brief

- Identify the applicable system requirements shown in chapter 'System Requirements (SR)' that provide technical security capabilities and meet the target security levels expressed by the SL-T vector.
- Identify available countermeasures.

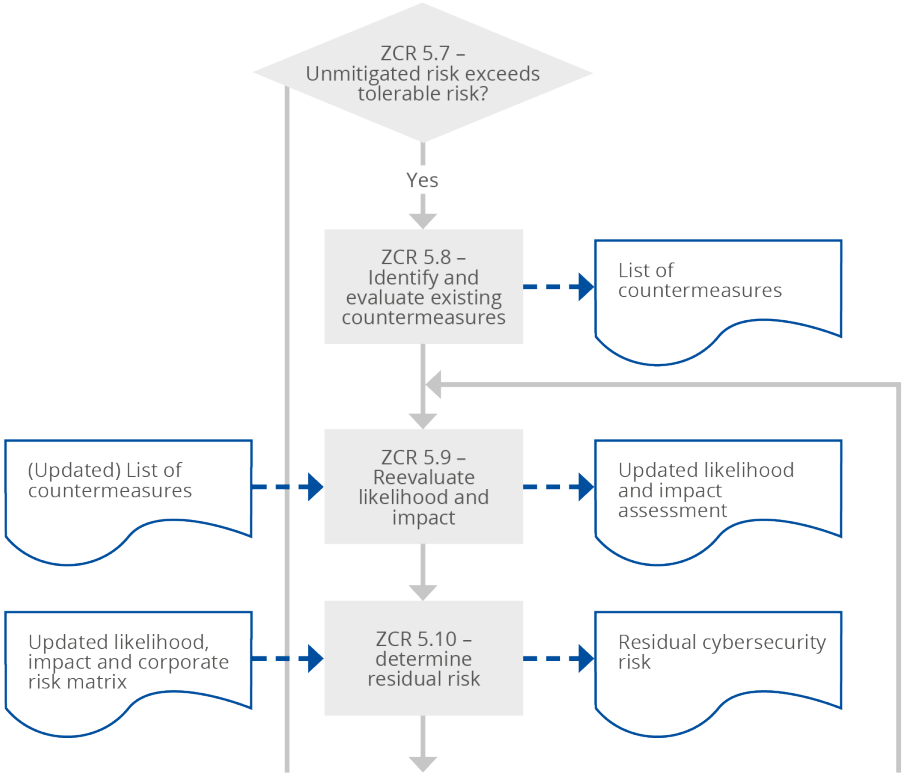
Output:

- a cybersecurity risk validated high level zone model;
- a cybersecurity risk validated zoning design report or other document;
- records of SL-T vector for each security zone;
- cyber-risk reports:
  - report of credible vulnerabilities from an independent professional reviewer
  - records of vulnerabilities,
  - fault or attack tree drawings with vulnerabilities,
  - asset register,
  - report of credible threats from an independent professional reviewer,
  - records of threat agents and actions,
  - fault or attack tree drawings,
  - assumed residual risk;
- required cybersecurity specifications (CRS) of the SuC.

3.5.4.3 Process step 5b: identify countermeasures

After determining security level targets, the existing countermeasures should be identified and evaluated. A zoning model with security boundaries (security gateways) should be available to identify available security functions or countermeasures and additional countermeasures that are missing.

Figure 19 Process of identifying countermeasures



3.5.4.4 Cookbook step 5b: identify existing countermeasures

If the residual risk exceeds stakeholder expectations, it is necessary to find additional countermeasures to increase security maturity, reduce the likelihood of impacts or increase system resilience. The approach is to allocate cybersecurity requirements on subsystem or component level first and then refine by requirements.

Additionally, the issue of compensating countermeasures is discussed in the context of cybersecurity requirements, where these are needed to satisfy a cybersecurity requirement or a substitute one due to technical constraints or limitations. Compensating countermeasures are part of the next chapter ‘Process step 5.C: Determine residual cyber risk’.

Input

The complete requirements for all zones and conduits included should be documented in the notes on the SuC. These include:

- a cybersecurity risk validated high level zone model;
- a cybersecurity risk validated zoning design report or other document;
- a cyber-risk report with assumed residual risk;
- required cybersecurity specifications (CRS) of the SuC;
- the level of tolerable risk;
- directive from the stakeholder against a lower or higher assumed risk;
- records of SL-T vectors for each security zone.

Task: Identifying and evaluating existing countermeasures in a brief:

- Evaluate the effectiveness of existing technical countermeasures of systems and networks against the system requirements as identified.
- Record the existing countermeasures and their effectiveness in the risk report.

The key objective of this chapter is the identification (and structuring) of security requirements for zones and conduits of a given SuC to provide an acceptable level of protection from all identified threats and known vulnerabilities. The security requirements for a SuC are mainly based on the system security requirements with additional (company dependent) guidance for railway applications.

The following topics should be considered:

- system security requirements,
- apportionment of cybersecurity requirements,
- breakdown of system requirements to subsystem level,
- allocation of system requirements at component level,
- specific consideration for the implementation of cybersecurity requirements on components,
- the requirement to breakdown structures as verification,
- compensating countermeasures.

Output

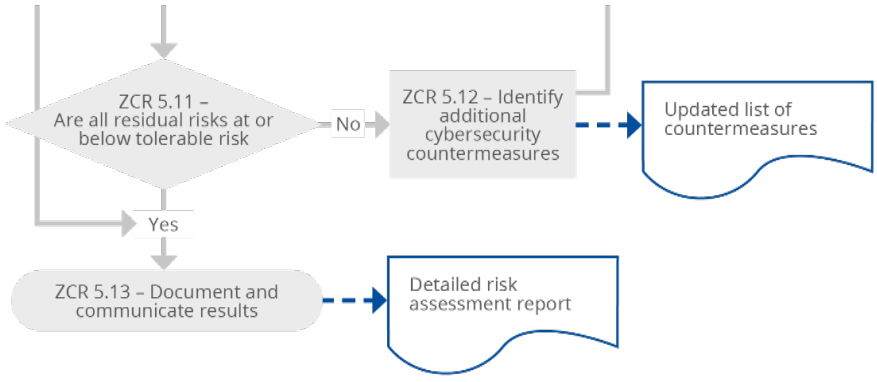
- list of compensating countermeasures,
- updated CRS with countermeasures and effectiveness.

Hint: the compensating countermeasures should be state-of-the-art, verified between asset owner and system vendor and approved by the system vendor.

3.5.4.5 Process step 5c: determine residual cyber risk

After identifying and evaluating existing countermeasures, the residual cyber risk rating taking existing countermeasures into consideration should be determined.

Figure 20 Process of verifying residual risk against tolerable risk



3.5.4.6 Cookbook step 5c: security measures for identified zones and conduits – how to protect or mitigate risk

The second approach about countermeasures is based on the difference between unmitigated cybersecurity risk and acceptable risk. It must be mentioned, as a precondition, that the zones and conduits to be assessed by a detailed risk assessment should have reached a certain level of maturity in their architecture and possibly their (planned) implementation. Generally, the second approach leads to a more appropriate SL-T value but takes more effort. Generally, the

detailed risk assessment described here is proactive, i.e. it is not triggered by an incident or vulnerability.

Input

The input to determine the residual cyber risk rating is:

- the risk report (including the level of tolerable risk),
- a cybersecurity risk validated high-level zone model,
- a cybersecurity risk validated high-level zoning design report or other document,
- a list of compensatory countermeasures,
- approvals from system vendors concerning the mitigating countermeasures.

Task: determining residual cyber risk rating in a brief

- Estimate the credible worst-case consequences and likely descriptions in accordance with the enterprise risk management system.
- Determine the residual cyber risk in accordance with the enterprise risk management system focusing on:
  - cybersecurity cases,
  - cybersecurity verification,
  - cybersecurity integration and verification,
  - assessment of results,
  - cybersecurity validation,
  - cybersecurity system acceptance,
  - independence,
  - objectives.
- Record the residual consequence and likely descriptions and residual cyber risk in the risk report.

Note: the residual cyber risk relates at this point to the ‘current residual risk’.

Output

The output from determining the residual cyber risk rating includes:

- risk report with residual consequence and likelihood descriptors and residual cyber risk.
- required cybersecurity specifications (CRS) of the SuC

The final step of the detailed risk assessment is to collect the cybersecurity requirements for a zone or conduit related to all threats or vulnerabilities from the various sources:

- requirements stated by using codes of practice (for threats covered by this principle);
- requirements from required cybersecurity specifications for applicable reference systems (for threats covered by this principle);
- requirements of IEC 62443-3-3 for the derived SL-T for the remaining threats arising from an explicit evaluation of risk.

In some cases, the requirements may arise from a single source, e.g. if a code of practice or a reference system is similar to a zone or conduit, but in general requirements from different sources need to be aligned.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6 AND 9

Residual risk? What risk remains? To be 100% secure is not possible from the technical point of view, and from the economic point of view it would be a financial nightmare.

Note: we can't eliminate security risks completely. A residual risk is always present.

The stakeholder and responsible asset owner should confirm all results and measures of risk analysis. They must decide whether the residual risk is too high (step back in the zoning process ZCR 5 – mitigating countermeasures) or whether the risk is tolerable.

3.5.5 Domain specific guidance

3.5.5.1 Signalling
No deviations.

3.5.5.2 Rolling stock
No deviations.

3.5.5.3 Fixed installations

Hint: more zones and independent firewalls ensure higher resilience, which results in lower residual risk for each zone.

3.5.5.4 Office and business
No deviations.

Note: internal networks, also gateways to external networks, might be down should a cybersecurity problem arise or there is a cyberattack. In such cases, it can happen that access to emergency documents or devices and network information (Chapter: DOCUMENTATION OF CYBERSECURITY REQUIREMENTS) is not possible via the network.

It can be useful to have a special isolated zone in the company crisis-management environment that collects all information during normal operations, but can act locally and offline in case of a network shutdown.

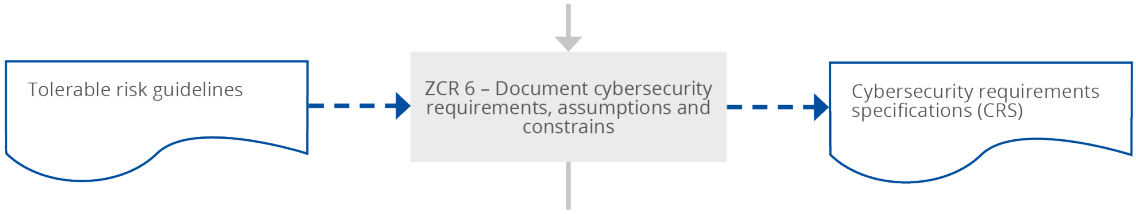
3.6 DOCUMENTATION OF CYBERSECURITY REQUIREMENTS (ZCR 6)

Guiding questions. How can we ensure that a complete change of the project team does not result in the loss of all knowledge? How should we document our results?

3.6.1 Process

The last 'project step' in the zoning process is the documentation. Cybersecurity is a part of the fast-changing digital environment. That means that incidents and hazards are changing, and measures must be modified. Documentation is one of the most overlooked processes. Nevertheless, should incidents occur, it is very important to have an overview of devices, firmware, models and software that is quickly accessible to plan the next operating steps or trigger crisis management if necessary

Figure 21 Documenting cybersecurity requirements (ZCR 6)



3.6.2 Design information

Collect all information's from 'living systems' instead of archive documents as far as possible.

3.6.3 Additional guidance

3.6.3.1 Cookbook step 6: documentation

Input:

- Functionally validated railway system **final zone model** and high-level documentation of:
  - organisational SuC (or 'subsystem' to prevent misunderstandings with technical SuC),
  - zones in the organisational SuC,
  - technical SuC such as interlocking systems or substations,
  - communication scheme on a high level with conduits and boundaries,
  - location and type of security gateways,
  - risk analysis from all zones and conduits with external networks (Internet, partner companies etc..);
- Functionally validated zone criticality (ZC) levels and a communication matrix (CM);
- A zoning design report;
- A threat landscape.

Task

- Collect all information into a well-known place or systems such as a risk management tool.
- Structure it for cyclic internal review or external (NIS) audit.

Output

- Actual documentation of zones, designs, communications, demands, measures and residual risk that can be found very quickly.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4

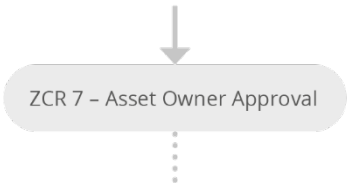
3.7 APPROVAL (ZCR 7)

Guiding question. When is the work finished? What must be done in order to get approval for the system?

3.7.1 Process

This last step is the formal agreement and approval by all participants, stakeholders, duty holders etc to commit to the final zone model, the (mitigating) countermeasures and the residual risk. If resources run out during migration, it results in two weak environments, higher complexity and a lot of temporary solutions. This culminates in an unknown system overall and higher risk.

Figure 22 Asset owner approval (ZCR 7)



SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	CHAPTER 6.4

3.7.2 Additional guidance

3.7.2.1 Cookbook step 7: documentation

Input

- final zone model,
- communication flow,
- data flow restrictions,
- secure and alternative ways to maintain the systems,
- planed cost, time and resources.

Task

This approval and commitment is the basis for planning, timing, internal and external human resources, and financial resources and the ‘Go’ for planning migration operations, especially where contingency measures are required for 24/7 operations.

Output

- start of operational part of the zoning project,
- HR and financial plan for each entity,
- aligned migration plan for each system group or zone,
- detailed migration plan with system vendors,
- possible breakdowns during migration identified,
- maximum downtime for operation identified,
- define process to enable communication on security gateways,
- TCO Cost.

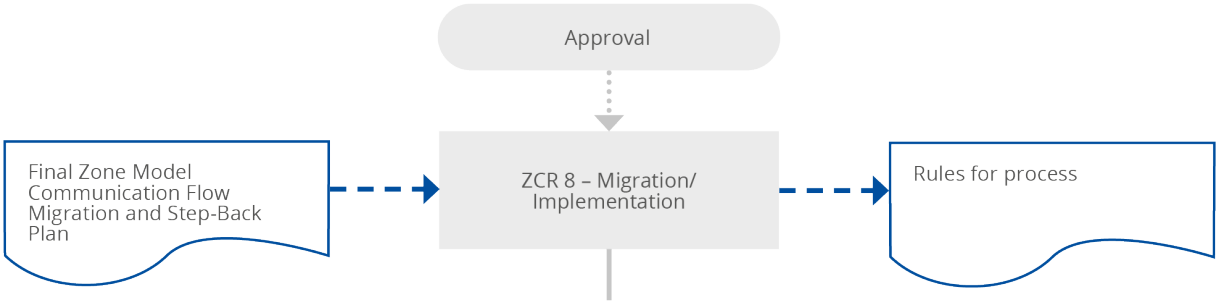
3.8 MIGRATION (ZCR 8)

Migration is not a part of the (planning) zoning process but is part of the overall zoning project. This step is only placed here to keep it in mind; however no details are described here. When this step begins, the theoretical part of zoning is over. From this moment, despite the pre-work

results of ZCR1 to ZCR 7, a lot of challenges will arise during migration in real 24/7 operations. Take care that fall-back plans are ready.

3.8.1 Process

Figure 23 Migration and implementation process (ZCR8)



3.8.2 Design information

No special information.

3.8.3 Additional guidance

3.8.3.1 Cookbook step 8: migration

Input

- final zone model
- communication flow
- detailed migration plan for each zone, as agreed with stakeholders, asset owner, operator and system vendor.

Task

Migrate systems and devices.

Hint: if something can happen – it will happen. Have a backup plan for each migration concept should migration fail in order 'to be able to reverse all steps taken'.

Output

- a zoned and secure railway network.

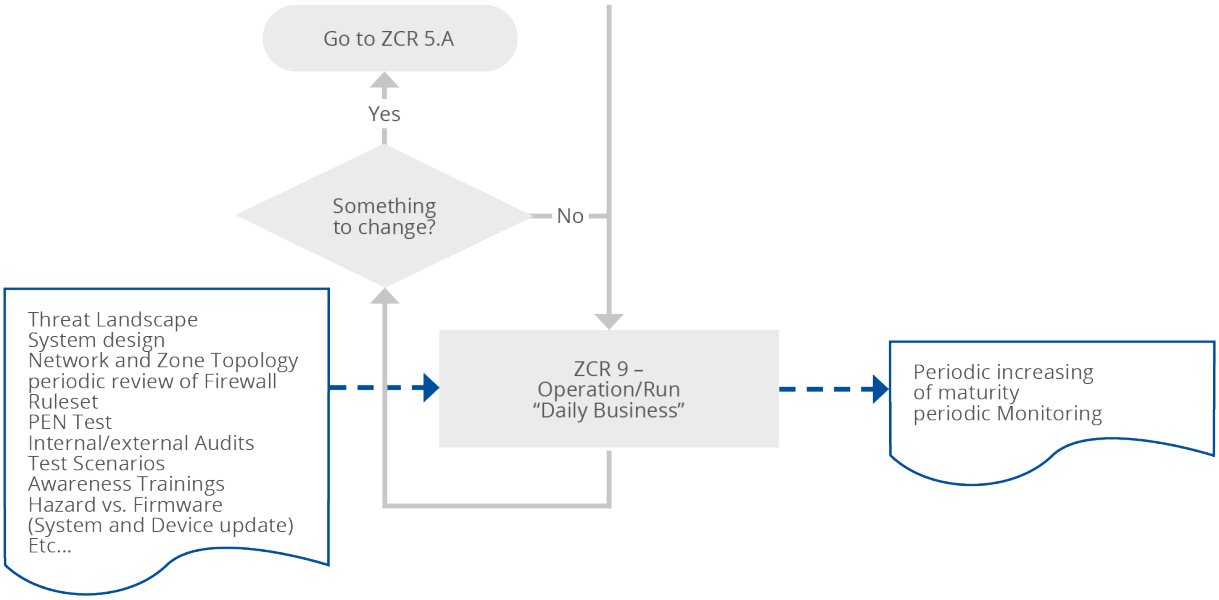
3.9 OPERATION / RUN (ZCR 9)

Guiding question. What will I have to do in order to keep my system in a safe and secure state, after it has been set into operation? What activities should be performed in order to detect and mitigate attacks?

3.9.1 Process

After migration all devises and systems, the final and endless process of 'run' ('daily business') starts. This step is only placed here to keep it in mind; however, no details are described here.

Figure 24 Operation/Run process (ZCR9)



3.9.2 Design information

If the next two 'monitor and review' steps result in new mitigating measures being needed or changing the system design or architecture of the network becomes necessary, refer to chapter 3.5 (Detailed Risk Assessment ZCR5).

3.9.3 Additional guidance

3.9.3.1 Cookbook step 9a: monitor and review threats

The continuous monitoring and reviewing during the run process are performed in the 'operate and maintain' stage of the asset lifecycle. These activities support submissions to configuration management unless a tailored application has been approved as defined. Each of the processes within continuous monitoring and reviewing is explained in the following chapters.

Input:

- records of criticality ratings for each process or utility area and the SuC;
- records of threat agents and actions;
- published security advisories, such as from ENISA, BSI, NIST or national government sites;
- security advisories from product suppliers;
- historical data of security events.

Process

- Check the environment and the monitoring system periodically.
- Install automatic notification systems should something happen and do all the things that a network operator would do. Have a look at some hints on the process found in figure 25 in Chapter 3.9.1
- Monitor advisories and historical data for new and changed threats at least every day.
- Review threats and scheduled maintenance activities to treat new and changed threats.
- Repeat the detailed risk assessment for each new or changed threat and at least annually.

Output:

- a zoned and secure railway network;
- schedule of maintenance activities.

3.9.3.2 Cookbook step 9b: monitor and review vulnerabilities

This process in continuous monitoring and reviewing is the monitoring and reviewing of new and changed vulnerabilities.

Input

- records of criticality ratings for each process or utility area and the SuC;
- records of vulnerabilities;
- published security advisories, such as from ENISA, BSI, NIST or national government sites;
- security advisories from product suppliers;
- historical data of security events.

Process

- Monitor advisories and historical data for new and changed vulnerabilities at least every day.
- Review vulnerabilities based on their common vulnerability scoring system (CVSS).
- Schedule maintenance activities to treat new and changed vulnerabilities within a defined period depending on the critically of the zone (ZC).

Output

- schedule of maintenance activities;
- a zoned and secure railway network.

Hint: if something can happen – it will happen. Have a crisis plan ready for each SuC.

4. LEGACY SYSTEMS

The system lifecycle and the high cost of OT devices results in a brownfield operation. This brownfield environment is a mix of new devices in green-field projects, which are integrated into existing monitoring or control/SCADA systems that worked with older legacy systems.

- Railways always have legacy systems.
- Legacy systems will be part of our daily business in the future.
- Legacy systems are not made less secure through the use of mitigating measures.

There are many ways to make legacy systems secure. They are dependent on the process and the functionality of the system. One possible easy way is to handle them like all other 'device-groups'. This means to identify them and give them their own zones with defending firewalls on the security devices on the conduit as described in the 'Steps' of this cookbook.

More information can be found in the Annexes in CLC/TS 50701:2021.

SOURCE	REQUIREMENTS AND REFERENCE
CLC/TS 50701:2021	ANNEX B

TP-06-22-138-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

978-92-9204-571-
510.2824/761090