OCORA

Open CCS On-board Reference Architecture

Project Cybersecurity Management Plan

Document ID: OCORA-TWS06-010

Version: 1.00

Release: Delta

Date: 30.06.2021

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Delta Release	RMe	30.06.2021

Table of contents

1 Introduction 10

1.1 Purpose of the Document 10
1.2 Applicability of the Document 10
1.3 Context of the Document 11

2 System under Consideration (SuC) 12

3 Today's Situation of Security 13

3.1 General Railway Operation 13
3.2 Rolling Stock 13
3.2.1 General 13
3.2.2 Architecture of today's OBU solution 14

4 Normative Background 15

4.1 General 15
4.2 Safety and Security 18
4.2.1 Achievement of the Safety Level depending on Security 19
4.2.2 Safety Standards and their limited Security Content according to prTS 50701 19
4.2.3 Security Impact on Availability and Integrity 20
4.2.4 Consequences 21
4.3 RAM and Security 22

5 Policy and Strategy for achieving Security 23

5.1 Security Protection Goals 23
5.1.1 No "Safety" Incidents 23
5.1.2 ISMS and Controls 23
5.1.3 Financial Viability 24
5.1.4 Prevent Blackmail 24
5.1.5 Train Delay 24
5.1.6 Maximal Total Failure Tolerance 24
5.1.7 Maximal Partial Operation Tolerance 24
5.2 Security Principles 24
5.2.1 Secure by Design 24
5.2.2 Defence in Depth 25
5.2.3 Detectability (Logging & Monitoring) 25
5.2.4 Design for Security Automation 25
5.2.5 Secure by Default 25
5.2.6 Simplicity over Complexity 26
5.2.7 Assume Failure & Compromise 26
5.2.8 Fail Safe and Secure (Graceful Degradation) 26
5.2.9 Usability & Manageability 27
5.2.10 Open Design 27
5.2.11 Zero Trust 27
5.2.12 Least Privilege 28
5.2.13 Design Security for Safety 28
5.2.14 Design Security for Innovation 28

5.2.15 Design Legacy System Inclusion 28
5.2.16 Heterogeneity for Security 29
5.3 Security Guidelines 29
5.3.1 Dynamic Security 29
5.3.2 Demand and Promote 29
5.3.3 Industrial Collaboration 29
5.3.4 Supply Chain Security 29
5.3.5 Support Standardization 30
5.3.6 Build on available Efforts 30
5.3.7 Advanced Availability and Robustness 30
5.3.8 Accountable Operation and SIEM Capability 30

6 Preliminary Analysis of Security Implications 31

6.1 Results of the analyse from today's Security 32
6.1.1 Architectural deficits on trains 32
6.1.2 Physical security on trains 32
6.1.3 Interoperability of the trains 32
6.1.4 Confidentiality of data on trains, missing basic communication confidentiality 32
6.1.5 In general, poor security level in almost all disciplines on trains 32
6.1.6 Low Resilience against advanced or targeted attacks 32

7 Planning of Security Activities 33

7.1 High Level Documentation Overview 33
7.1.1 CS Overview 33
7.1.2 CS Strategy 34
7.1.3 CS Guideline 34
7.1.4 Project Cybersecurity Management Plan 34
7.1.5 CS Concept 34
7.1.6 Cybersecurity Requirements Specification 34
7.2 Cybersecurity Activities Management 35
7.2.1 Project Organization 35
7.2.2 Role and responsibilities 35
7.2.3 Interface with other stakeholders 35
7.2.4 Key Milestones 35
7.3 Security Engineering Process 36
7.3.1 Introduction 36
7.3.2 Process Evaluation 38
7.3.3 Security Risk Assessment Structure 38
7.3.4 Security Risk Assessment Approach 38
7.4 Ensuring appropriate Degree of personal Independence 39
7.5 Security related Documentation 39
7.6 System Design 39
7.6.1 Identify assets for essential functions 40
7.6.2 Apportionment to zones and conduits 40
7.6.3 Verify and leverage possibilities to optimize security by design 40
7.6.4 Refine normative requirements to SuC specific requirements 41
7.6.5 Specify Requirements for secure disposal and renewal 41
7.6.6 Assign technical security requirements to components 41
7.7 Risk Management 42

7.7.1 CIA-PNR analysis, classification, and categorization 42
7.7.2 Challenges & approaches 43
7.7.3 Definition & update of threat landscape 43
7.7.4 Impact analysis for the SuC 44
7.7.5 Definition of risk acceptance criteria and scaling of risk matrix 45
7.7.6 Refinement of initial impact assessment in threat log (scenarios) 45
7.7.7 High-level, zone-based risk analysis 45
7.7.8 Detailed risk analysis 45
7.7.9 Definition of organizational and physical requirements and/or application conditions 46
7.7.10 Component based risk analysis update and definition of compensating countermeasures 46
7.8 Identification, Coordination, and resolution of conflicts 46
7.8.1 Identify necessary contacts to analyse and resolve conflicts 47
7.8.2 Analyse top impacts for potential conflicts 47
7.8.3 Identify and document risks with potential implications in other fields 47
7.9 Process and infrastructure for testing and integration 48
7.9.1 Specify testing infrastructure and procedures throughout the lifecycle 48
7.9.2 Specify testcases for each cybersecurity requirement 48
7.10 Verification 49
7.11 Validation 49
7.12 Maintenance, Performance and Operation 49
7.12.1 Consider business continuity aspects (incl. incidence response and recovery) for the SuC 49
7.12.2 Plan for security monitoring and vulnerability management 50
7.12.3 Assign responsibilities for organisational and physical requirements 50
7.12.4 Establish third party management for security, including supplier security capabilities and support contracts 50

8 Further considerations for CENELEC phase 6-12 51

8.1 Ensuring appropriate degree of personal independence 51
8.2 Maintenance of security related documentation 51
8.3 System design 51
8.3.1 Analyse and identify updates to system design post implementation 51
8.3.2 Analyse security functionality and requirements coverage 52
8.3.3 Verify applicability of organizational and physical requirements and application conditions 52
8.3.4 Document and finalize Cybersecurity Case 53
8.4 Risk Management 53
8.4.1 Update risk analysis according to update of system design 53
8.4.2 Update risk management results 54
8.5 Identification, Coordination, and resolution of conflicts 54
8.5.1 Identify, document, and resolve conflicting measures and functional topics 54
8.6 Process and infrastructure for testing and integration 54
8.6.1 Update and apply defined procedures 55
8.6.2 Disposal of testing-infrastructure taking security criteria into account 55
8.7 Verification 55
8.8 Validation 55
8.9 Maintenance, Performance and Operation 56

8.9.1 Monitor development process and application conditions as they are developed 56
8.9.2 Removal of unnecessary software, hardware, and services 56
8.9.3 Configuration and qualification of security components 57
8.9.4 Strategy to maintain SuC in security conditions 57
8.9.5 Review and update business continuity aspects (incl. incidence response and recovery) for the SuC 57
8.9.6 Security and vulnerability monitoring 58
8.9.7 Data backup and auditing procedures 58
8.9.8 Maintenance of restrictive access authorizations 58
8.9.9 Application of strategy to maintain SuC in security conditions 59
8.9.10 Disposal of components taking security criteria into account 59

Table of figures

Figure 1 CCS On-board 12
Figure 2 Architecture of planning OBU 14
Figure 3 Railway standards 15
Figure 4 Development of prTS 50701 15
Figure 5 V-Cycle EN 50126 16
Figure 6 prTS 50701 Statements of Impact 19
Figure 7 Security document structure and timeline 33
Figure 8 Cybersecurity Assurance Process according to prTS 50701 34
Figure 9 Relations of EULYNX, RCA and OCORA 35
Figure 10 Process Interaction 36
Figure 11 Workstream activities 38
Figure 12 CIA-PNR classification 43

Table of tables

Table 1 Tiers 17
Table 2 Maturity Level 17
Table 3 IT-Security requirements 21
Table 4 Security Levels 22
Table 5 Security topics at railway systems 31
Table 6 Mapping Security Model to EN 50126 Phase Model (phase 1-5) 37
Table 7 Advantages and disadvantages of static and functional approaches 38
Table 8 Personal independence 39

Table 9 Security documentation 39
Table 10 System Design 39
Table 11 Identify assets for essential functions 40
Table 12 Apportionment to zones and conduits 40
Table 13 Verify and leverage possibilities to optimize security by design 40
Table 14 Refine normative requirements to SuC specific requirements 41
Table 15 Specify Requirements for secure disposal and renewal 41
Table 16 Assign technical security requirements to components 41
Table 17 Risk Management 42
Table 18 CIA-PNR analysis, classification, and categorization 42
Table 19 Classification Levels 43
Table 20 Challenges & approaches 43
Table 21 Definition & update of threat landscape 44
Table 22 Impact analysis for the SuC 44
Table 23 Refinement of initial impact assessment in threat log 45
Table 24 High-level, zone-based risk analysis 45
Table 25 Definition of organizational and physical requirements and/or application conditions 46
Table 26 Component based risk analysis update and compensating countermeasures 46
Table 27 Identification, Coordination, and resolution of conflicts phase 1-5 46
Table 28 Identify necessary contacts to analyse and resolve conflicts 47
Table 29 Analyse top impacts for potential conflicts 47
Table 30 Identify and document risks with potential implications in other fields 47
Table 31 Process and infrastructure for testing and integration 48
Table 32 Specify testing infrastructure and procedures throughout the lifecycle 48
Table 33 Specify testcases for each cybersecurity requirement 48
Table 34 Cybersecurity Verification phase 1-5 49
Table 35 Cybersecurity Validation phase 4 49
Table 36 Maintenance, Performance and Operation phase 3-5 49
Table 37 Consider business continuity aspects for the SuC 49
Table 38 Plan for security monitoring and vulnerability management 50
Table 39 Assign responsibilities for organisational and physical requirements 50
Table 40 Establish third party management for security, including supplier security capabilities and support contracts 50
Table 41 Ensuring appropriate degree of personal independence phase 6-12 51
Table 42 Maintenance of security related documentation phase 6-12 51
Table 43 System design phase 8-10 51
Table 44 Analyse and identify updates to system design post implementation 52
Table 45 Analyse security functionality and requirements coverage 52
Table 46 Verify applicability of organizational and physical requirements and application conditions 52
Table 47 Document and finalize Cybersecurity Case 53
Table 48 Risk Management phase 8-11 53

Table 49 Update risk analysis according to update of system design 53
Table 50 Update risk management results 54
Table 51 Identification, Coordination, and resolution of conflicts phase 6-12....54
Table 52 Identify, document, and resolve conflicting measures and functional topics phase 6-12....54
Table 53 Process and infrastructure for testing and integration 54
Table 54 Update and apply defined procedures 55
Table 55 Disposal of testing-infrastructure taking security criteria into account....55
Table 56 Cybersecurity Verification phase 6-12 55
Table 57 Cybersecurity Validation phase 9....55
Table 58 Maintenance, Performance and Operation phase 6-12....56
Table 59 Monitor development process and application conditions as they are developed....56
Table 60 Removal of unnecessary software, hardware, and services 56
Table 61 Configuration and qualification of security components 57
Table 62 Strategy to maintain SuC in security conditions....57
Table 63 Review and update business continuity aspects for the SuC 57
Table 64 Security and vulnerability monitoring 58
Table 65 Data backup and auditing proceduresMaintenance of restrictive access authorizations 58
Table 66 Maintenance of restrictive access authorizations 58
Table 67 Application of strategy to maintain SuC in security....59
Table 68 Disposal of components taking security criteria into account 59

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.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-011 – Problem Statements

[7] OCORA-BWS03-010 – Introduction to OCORA

[8] OCORA-BWS08-010 – High Level Methodology

[9] OCORA-TWS01-010 – System Architecture

[10] OCORA-TWS06-020 – (Cyber-) Security – Guideline

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

[12] EN 50128:2012 - Railway applications – Communication, signalling and processing systems – Software for railway control and protection systems

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

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

[15] prTS 50701 - Railway application - Cybersecurity

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

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

[18] ISO 27005 - Information security risk management

[19] ISO 27000 - Information security management systems – Overview and vocabulary

[20] ISO/IEC 17799 - Information Security Standard (valid until June 2007)

[21] OCORA-TWS01-100 – CENELEC Phase 1 – Concept

[22] OCORA-BWS05-010-Delta – Road Map

1 Introduction

1.1 Purpose of the Document

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader will gain insights regarding the topics listed in this chapter 1.1, and is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete CCS system, or also for CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

The purpose of this document is to cover the CENELEC Phase 1 activities defined in prTS 50701 [15]. It presents the frame of the OCORA initiative and project through the following elements:

- Fulfill the requirements of the standards for the creation of a Project-Cybersecurity-Management-Plan
- Identification of the Security requirements from past experiences and today's solution
- Presentation of the Security policy used within OCORA
- Cover the relevant security-related activities for the railway application lifecycle according to EN 50126-1 [11].
- Show the cybersecurity strategy for OCORA

The project cybersecurity management plan (PSMP) defines the cyber-security related tasks. They shall be carried out throughout the whole lifecycle of a system according to the CENELEC methodology described in EN 50126-1 [11]. It is a living document which is updated frequently, after new insights have come to the knowledge of the respective project or operations team.

This document is intended to provide an overview of the topic of security as well as the related objects and interfaces (e.g.: Safety, RAM and System Architecture). It should serve as the rough guidelines for the creation of concrete guidelines to carry out a security threat analysis according to the standards.

This CENELEC development is decorrelated from the different releases of OCORA. So far, Alpha, Beta and Gamma releases are considered.

1.2 Applicability of the Document

This document is developed as part of the OCORA project of the OCORA initiative. This document is valid for the OCORA project and describes the (cyber-)security related activities for the OCORA tailored lifecycle of the system according to EN 50126-1 [11].

The authors are responsible for creating, updating, and managing of this document.

The validity of this document is regulated at least for the entire duration of the project and at most by the defined retention requirements from the project.

The document represents the current state of the document and if necessary, it will be further developed in consecutive releases.

1.3 Context of the Document

This document is published as part of the OCORA Delta release, together with the documents listed in the release notes [1]. It is the first release of this document which will be further developed in consecutive releases.

Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 System under Consideration (SuC)

The system under consideration is the CCS onboard reference architecture designed by the OCORA initiative outlined in Figure 1.

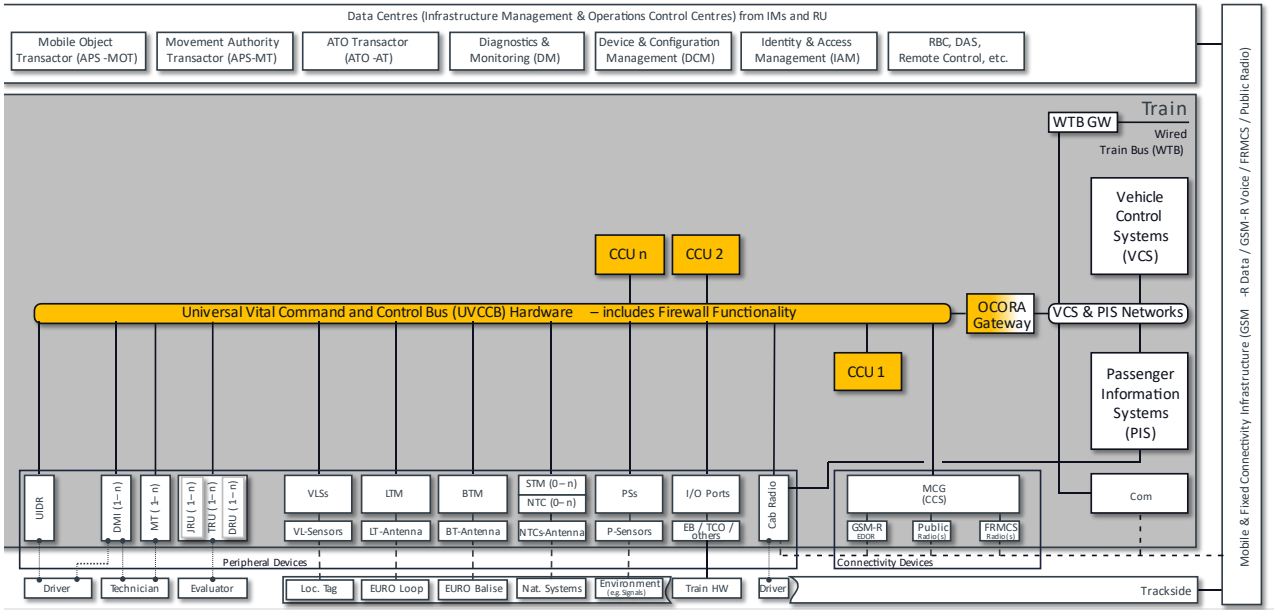

Figure 1 CCS On-board

A detailed description of the architecture is presented in OCORA-TWS01-010 – System Architecture [9].

The document CENELEC phase 1 – Concept (CP1) [21] from EN 50126-1 [11] describes the following:

- Scope, context, and purpose of OCORA (initiative, program, project, deliveries)
- Scope, context, and purpose of the SuC
- Presentation of the environment of the SuC
- Identification of the RAMSS requirements from past experiences
- Presentation of the RAMSS policy used within OCORA
- Presentation of the safety legislation
- List of assumptions and justifications

Note:

The chapters from the Concept (CP1) [21] from EN 50126-1 [11] indicated with RAMSS include the RAM, safety, and security related content.

Topics already covered by the OCORA Concept (CP1) [21] are not presented in this document.

The exact system definition including system boundaries, component and subsystem definitions will be available in CENELEC phase 2 - System Definition (CP2) according to EN 50126-1 [11].

3 Today's Situation of Security

The primary goal of security in connection with systems or applications relevant for safety critical and availability critical operations must be to ensure that security incidents do not result in safety, operational nor service incidents and that a minimized risk regarding safety and service is guaranteed.

Because of the growing digitalization and automation of processes, it is now necessary to implement protective, detective, and reactive measures against cyber-attacks, to ensure reliable railway operations.

For the most recent projects and projects in conception, cybersecurity is now more considered, and some enhancement is in progress, accomplished by creating and applying of international standards like the prTS 50701 [15] and the IEC 62443 [16] and with the related standardization initiatives like RCA (Reference CCS Architecture) and EULYNX.

3.1 General Railway Operation

The whole railway operation system has grown over time and in technology. It is a patchwork of technologies and standards with many elements spread over a whole country and with interfaces and relations to neighboring countries.

The high number of interfaces and interdependencies pose a high risk for cross company infections and incidents. Old analogue systems, electronic Interlockings and digital control are all existing side by side. Since security always depends on the weakest element in the chain, the vulnerabilities are manifold.

The current approach in the railway industry of safety and operation first, also results in gaps from the security point of view.

With the actual strongly increased number of cyber-attacks worldwide and the simple possibilities in organizing vandalism over social channels, the rail system has become very vulnerable to intentionally motivated attacks.

Exactly this has been shown by the project Honeytrain[1] technology exposed to the internet. In a timeframe of only six weeks over 2,7 million attacks have been identified on the systems of a simulated railway operation. This means that every minute 45 attempted attacks have been logged and approximately one attack was detected from almost every country in the world.

Four of these attacks did manage to get access to sensitive systems like the HMI (human machine interface) which is used to monitor and control interlocking functions like moving switches, setting train routes, controlling signals and block bridging. Devastating damage could happen if a hacker with bad intents takes over the controlling functions of interlockings.

In 2017 the ransomware WannaCry[2] infected 450 computers at DB and led to the failure of display boards at many train stations, video surveillance systems and a regional control center in Hanover.

Railway is usually one of the biggest businesses in a country and has public access. Which means persons like passengers are usually just one door away from technical railway equipment. Due to the size, passenger volume and high financial flow, a rail operator is an attractive target for attacks and needs to be secured.

3.2 Rolling Stock

3.2.1 General

The increasing communication of components and subsystems results in more and more interfaces and points of contact between systems that are required for a modern railway operator. Currently, there are no adequate and commonly used security solutions in place to protect against unauthorized access or to completely prevent unauthorized interventions and attacks. This results in a steadily growing attack surface for internal and external attacks on safety-relevant systems of a railway operator.

[1] Source: https://news.sophos.com/de-de/2015/09/17/projekt-honeytrain-hackerwork/ and https://presselounge.tc-communications.de/media/files/Hontrain-WP_Sophos_Textfinal-layouted.pdf

[2] Source: https://de.wikipedia.org/wiki/WannaCry

In one of the attacks detected during the Honeytrain[3] project it was possible to activate the front lights of one simulated train. A command line was started, two PINGs were executed, and the execution program opened. It was found that the security configuration of industrial components was read via a central tool, and the settings were exported. This points out that trains can also serve as a target for cyberattacks.

Cybersecurity considerations also apply to rolling stock. A modern train is effectively a mobile data center, communicating with the trackside equipment, the depot, the operational control center, traincrew, and the passengers. These information flows offer the hacker several potential entry points, all of which need to be carefully managed to mitigate the security threat. A further evolution of onboard technology can be expected, which will in fact increase the number of possible security threats:

- Harmonized onboard computing platform with the option to do updates and patches (at least of non-safety-relevant components) remotely
- Introduction of new onboard sensors and subsystems in the context of more automation
- Increased standardization of onboard components and interfaces

Interoperability of trains (e.g., train to ground communication, as well as communication with stations and dispositional systems; and key exchange and how to handle this all in an interoperable way) needs to be clarified and established at an international level. Even when crossing a border, it must be ensured that security and safety are fully guaranteed.

Another critical gap is the physical security of locomotives. Locomotives and train compositions are sometimes left unlocked. Apart from that, it is currently also possible to use the simplest means to gain unauthorized access to a driver cabin or to important control components of the trains. A concept, which ensures physical access restrictions, even when the vehicle is disconnected, should be developed, and implemented to secure the IT systems in the vehicles.

3.2.2 Architecture of today's OBU solution

The CCS vehicle architecture consists of all relevant hardware and software components that are required for the safe movement of a driven rail vehicle. This includes particular the following functions on the vehicle:

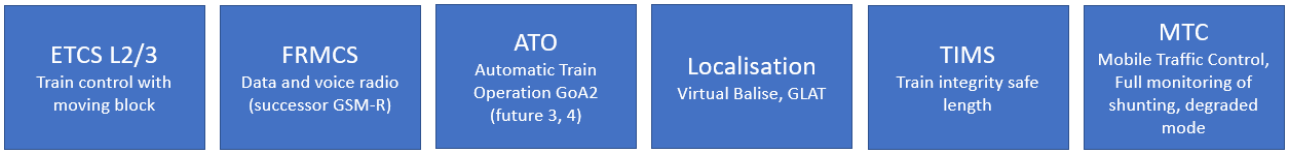

Figure 2 Architecture of planning OBU

Vehicles currently or soon in operation have different architectures and systems. On the one hand, this is because vehicles of several technology generations are in operation. On the other hand, in recent years the tenders have been designed in such a way that the architecture has largely been left to the vehicle suppliers. These circumstances mean that the life cycle costs for the fleets are disproportionately high due to the proprietary solutions and the corresponding specific interfaces between these systems since vehicle suppliers and system suppliers must be used again and again. Upgrades, expansions, and modifications are, if at all, only very costly to accomplish. In addition to the general technological developments and expansions, adjustments and / or additional equipment and systems will probably be implemented on the vehicle as part of the upcoming TSI standards. The aim is to find a solution that enables an open architecture that is as independent of the supplier as possible, or specifies which updates, expansions and adaptations to the interfaces, interface functions and (sub) systems should be controlled as simply and, above all, centrally as possible, and additionally one enables massive reduction in the effort required for approval.

[3] Source: https://www.railengineer.co.uk/2017/05/30/hacking-the-railway/ and https://presselounge.tc-communications.de/media/files/Hontrain-WP_Sophos_Textfinal-layouted.pdf

4 Normative Background

4.1 General

This chapter shows the fundamental basis for the security activities which must be followed during the development of security solutions.

The most important standards currently available for realizing security and safety related railway projects are EN 50126-1 [11], EN 50129 [13], EN 50159 [14], and IEC 62443 [16]. Figure 3 gives an overview and shows the partly overlapping in their aspects.

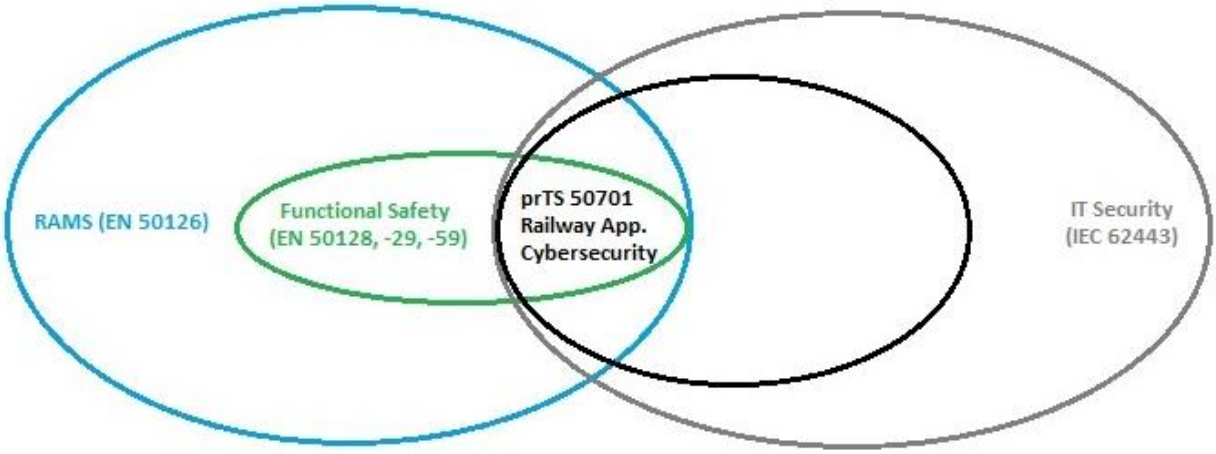

Figure 3 Railway standards

The standard prTS 50701 [15] combines the approaches from the CENELEC standard with the ones from the already established security standard IEC 62443 [16] (see Figure 4).

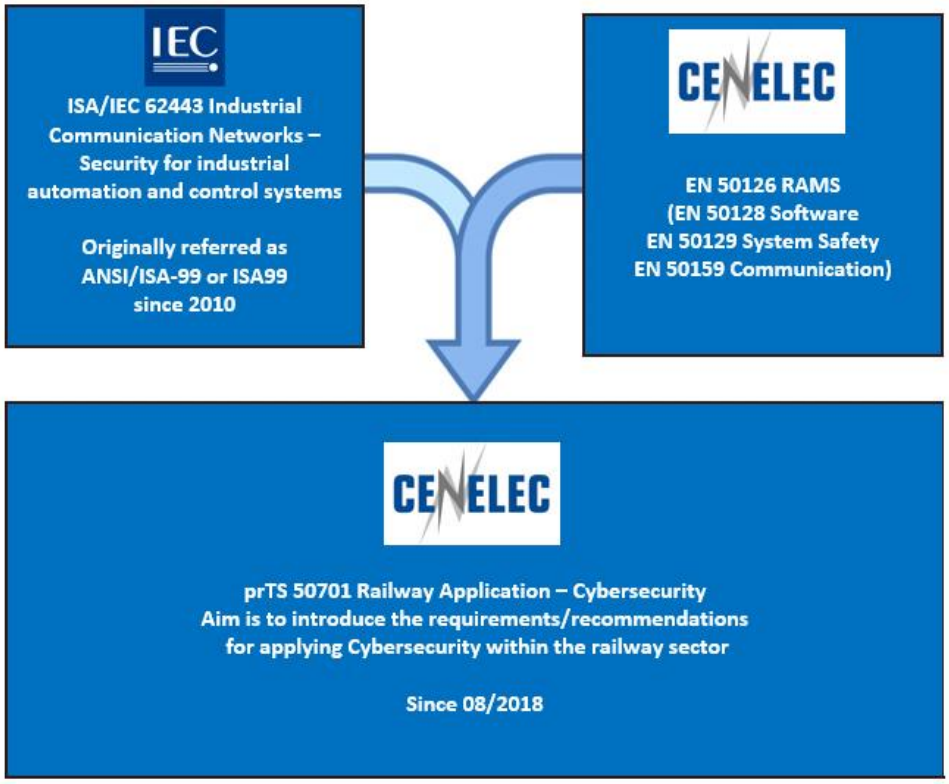

Figure 4 Development of prTS 50701

The base of prTS 50701 [15] is the V-Cycle (see Figure 5) from the CENELEC standard EN 50126-1 [11].

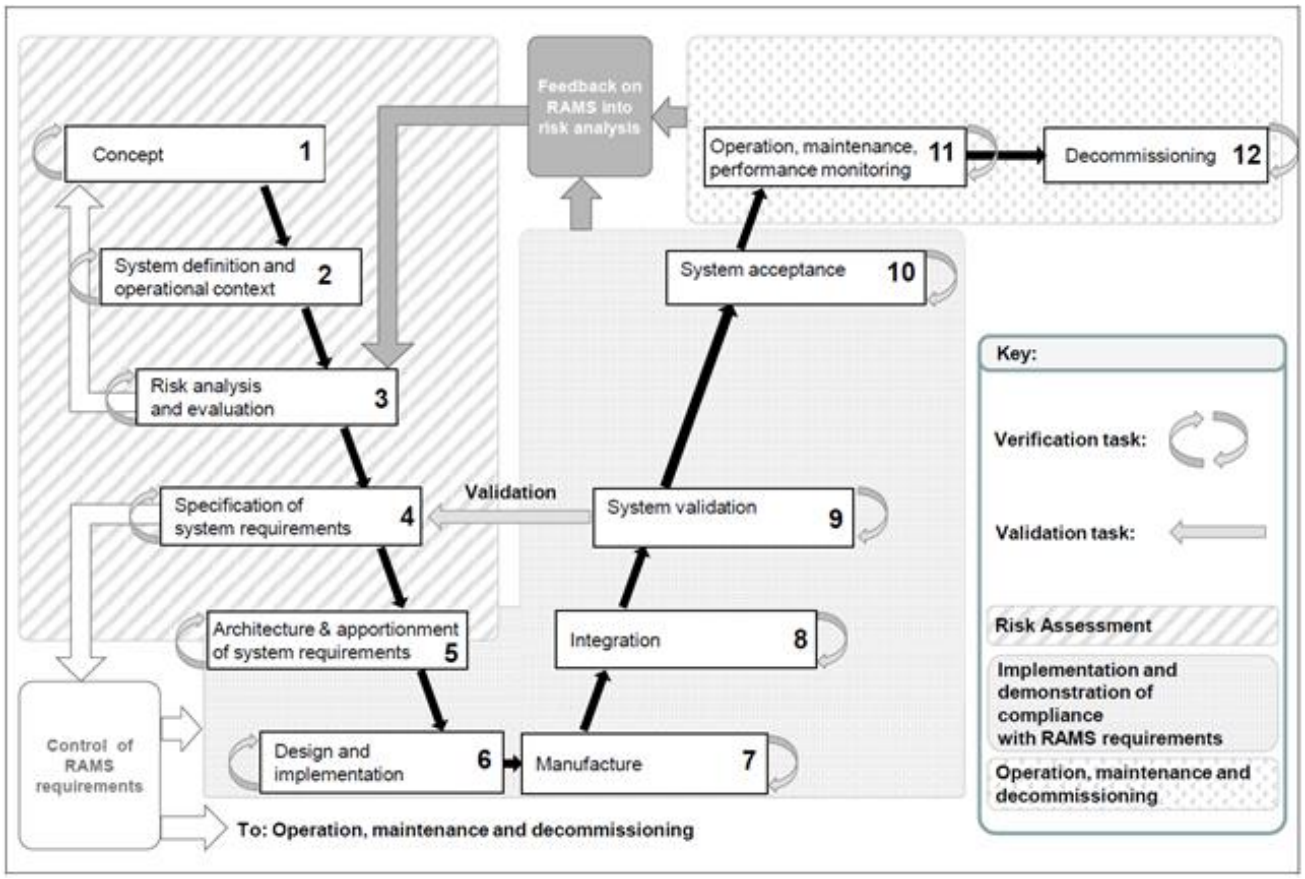

Figure 5 V-Cycle EN 50126

The V-model stands for verification and validation. Just like the waterfall model, the V-Shaped life cycle is a sequential path of execution of processes. Each phase can only be completed if the phase before it has already been completed. Testing of the product is planned in parallel with a corresponding phase of development. Requirements begin the life cycle model. A key aspect of this model is, that before development is started, a system test plan is created. The test plan focuses on meeting the functionality specified in the requirements gathering.

Advantages of V-model:

- Simple and easy to use
- Testing activities like planning and test designing happens well before coding to save time
- Proactive defect tracking (defects are found at an early stage)

Disadvantages of V-model:

- Very rigid and least flexible
- Software is developed during the implementation phase, so no early prototypes of the software are produced
- If any changes happen in midway, then the test documents along with requirement documents must be updated

More details about safety synchronisation and cybersecurity assurance are presented in the OCORA-TWS06-020 – (Cyber-) Security – Guideline [10].

The application of prTS 50701 [15] should be mandatory if security solutions are developed for safety related functions/systems. At the time of writing only a draft version of this standard is available, but the standard has already grown and evolved, and the final version will be published in July 2021.

Due to the circumstance that a lot of documentation and environmental work needs to be done to satisfy CENELEC standards an approach could be to separate the development of security solution for safety related functions/systems.

Based on a threat analysis, structural analysis that follows the architecture, followed by a risk analysis shall define the relevant Security Level (Table 4), TIER level (see Table 1) or Maturity Level (see Table 2). The NIST Cybersecurity Implementation Tiers are a scaled ranking system that describes the degree to which an organization exhibits the characteristics described in the NIST Cybersecurity Framework [17].

The application of the Security Levels is demonstrated in the document OCORA-TWS06-020 – (Cyber-) Security – Guideline [10].

Tier	Name	Explanation
1	Partial	Informal practices; limited awareness; no cybersecurity coordination
2	Risk Informed	Management approved processes and prioritization, but not deployed organization-wide; high-level awareness exists, adequate resources provided; informal sharing and coordination
3	Repeatable	Formal policy defines risk management practices processes, with regular reviews and updates; organization-wide approach to manage cybersecurity risk, with implemented processes; regular formalized coordination
4	Adaptive	Practices actively adapt based on lessons learned and predictive indicators; cybersecurity implemented and part of culture organization-wide; active risk management and information sharing.

Table 1 Tiers

In IEC 62443-4-1 [16] the maturity levels provide more details on how thoroughly a supplier has met these requirements. The maturity levels are based on the Capability Maturity Model Integration for Development (CMMI-DEV).

Maturity Level	Name	Description
1	Initial	Product suppliers typically perform product development in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency across projects and repeatability of processes may not be possible.
2	Managed	At this level, the product supplier has the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it. However, at this level, the organization does not have experience developing products to all the written policies. This would be the case when the organization has updated its procedures to conform to this document but has not yet put all the procedures into actual practice, yet. The development discipline reflected by maturity level 2 helps to ensure that development practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans. NOTE: At this level, the CMMI and IEC62443-4-1 [16] maturity models are fundamentally the same, with the exception that IEC62443-4-1 [16] recognizes that there may be a significant delay between defining/formalizing a process and executing (practicing) it. Therefore, the execution related aspects of the CMMI-DEV Level 2 are deferred to Level 3.
3	Defined (Practiced)	The performance of a level 3 product supplier can be shown to be repeatable across the supplier's organization. The processes have been practiced, and evidence exists to demonstrate that this has occurred. NOTE: At this level, the CMMI and IEC 62443-4-1 [16] maturity models are fundamentally the same, with the exception that the execution related aspects of the CMMI-DEV level 2 are included here. Therefore, a process at level 3 is a level 2 process that the supplier has practiced for at least one product.
4	Quantitatively Managed	At this level, IEC62443-4-1 [16] combines CMMI-DEV levels 4 and 5. Using suitable process metrics, product suppliers control the effectiveness and performance of the product and demonstrate continuous improvement in these areas.
5	Optimizing	See ML4

Table 2 Maturity Level

The prTS 50701 [15] standard describes how this is to be used in the railway environment. It is relevant for the entire life cycle for development and documentation.

This effort is needed because of the upcoming increase in security, which affects, among other things, the following topics:

- Physical security with protection against unauthorized access to driver's cabs, control components and bus systems.
- Secure architecture on the train with zoning, firewalling and authentication / authorization for all users and system components.
- Use of security hardened components on secure and current operating systems.
- Ensuring the integrity of all software and hardware components used. Protection against the introduction of third-party software packages, using back doors or even installing new hardware units or manipulating existing ones.
- Ensure periodic updates at defined time intervals to protect against dangerous security gaps (SW lifecycle, security patching).
- Securing of data and communication protocols with current technologies such as encryption, integrity checks and strong authentication.
- Securing wireless communication and access

4.2 Safety and Security

Security is a key element for providing safety. Ensured integrity of communication and systems directly influences safety decisions. Nevertheless, for handling the two differing topics efficiently safety and security needs to be layered. For approval reasons it is necessary to separate the security solutions as far as possible from safety aspects so that security updates shall not require a new safety certification. The “security as a shell” principle is to be the basis to achieve these design targets.

The timescales of safety / RAMS and security systems are different. The main reason for this is the procedures necessary for verifying safety and obtaining approval for operation from the authorities. Certain security measures may require fast action for remediation, however. This means that there is a fundamental conflict between security and safety (consider the example of patching a disclosed vulnerability in a safety-certified system).

There are three different philosophies to approach this problem:

- **Added security for safety:** Security may be "added" to a system under consideration by adding a component, e.g., a firewall. In this case, such a component may be considered as a tool (category T3) according to EN50128 [12]. (The purpose of the tool is to ensure a secure operational environment at runtime of the system under consideration.) The correctness of tools also must be verified with similar methods as for the "real", safety-relevant system under consideration. However, the main benefit of this approach lies in a decoupling of the system under consideration from the tools needed to build the SuC and in extension a decoupling of the lifecycles of SuC and tools.
- **Integrated security for safety:** Certain security features will have a close relation to the system under consideration. The patching is such an example. In this case security related features must be considered as part of the system and thus also as part of the safety case for the system. It is vital to design the system under consideration (and especially its security features) such, that the safety case does not have to be re-made every time a security function (like patching the system) is invoked. The main instrument to realize such functions in a robust way are requirements and application conditions. Requirements need to be exchanged back and forth between security and safety/RAMS at an early stage (phases 1-4) and the application conditions must combine both views (security and safety/RAMS) in phases 9 and 10. There are two kinds of application conditions:
  - **Security related application conditions (SecRACs):** These are the assumptions and conditions that need to be satisfied to mitigate risks. Correct handling of SecRACs is a precondition for secure implementation and operation. Example: The operator must always ensure hard drive encryption (Bit locker), even throughout maintenance.
  - **Safety-related security application conditions (SRSACs):** These are required for a safe operation of the SuC and shall be passed on to the Safety Case and the Asset Operator. Example: After patching the system, the operator must carry out a specified procedure to ensure, the system still behaves according to its specification and parameters do not leave predefined ranges.

- **Security for non-safety topics:** Certain security features will not have the purpose of providing a secure environment for a RAMS-relevant system but have other security implications like privacy. These security-features should be developed according to applicable codes of practice in the respective areas.

4.2.1 Achievement of the Safety Level depending on Security

Some recent incidents and analyses indicate that the vulnerability of IT systems in railway automation has been underestimated so far. Due to several trends, such as the use of commercial IT and communication systems or privatization, the threat potential has increased.

What distinguishes railway systems from many critical infrastructures is their inherent distributed and networked nature with thousands of track-kilometres for major operators, or even more. Thus, it is not economical to completely protect against physical access to this infrastructure and, consequently, railways are very vulnerable to physical denial-of-service attacks leading to service interruptions.

Another distinguishing feature of railways from other systems is the long lifetime of their systems and components. Current contracts usually demand support for at least 25 years and history has shown that many systems, e.g., mechanical or relay interlockings, last much longer. IT security analyses must consider such long lifespans.

Some of the technical problems are not railway-specific but are shared by a few other sectors such as Air Traffic Management. Publications and presentations related to IT security in the railway domain are increasing.

Some are particularly targeted at the use of public networks such as Ethernet or GSM/FRMCS for railway purposes, while others directly pose the question “Could rail signals be hacked to cause crashes?” While in railway automation harmonized functional safety, standards were elaborated more than a decade ago, up to now no harmonized international IT security requirements for railway automation exist.

It is obvious that in nowadays digitalized world, safety levels can only be achieved if the underlying security is on a level, that safety can trust on. But the needed level is not easily defined. So more detailed questions must be answered first.

4.2.2 Safety Standards and their limited Security Content according to prTS 50701

The new Standard prTS 50701 [15] that is about to be released states in a draft the following points on how to address security for safety. From a protection point of view the standard gives the following picture and principles for the consideration of the impact of security on safety:

Figure 6 prTS 50701 Statements of Impact

The prTS 50701 [15] standard defines the base principles how security (prTS 50701 [15]) and safety (EN 50126 [11]) must be handled. The statements of impact of security to safety lists the following:

- Principle 1: Safety and security are different and should be treated as such.
- Principle 2: The security environment shall protect essential functions, incl. safety.
- Principle 3: Threat & risk analysis is the main interface with safety analysis.
- Principle 4: Separate security and safety as far as possible but coordinate them effectively.
- Principle 5: Security shall be evaluated based on international standards, e.g., IEC 62443 [16].
- Principle 6: It is impossible to evaluate the security risk probabilistically.
- Principle 7: Safety and security target measures shall not be coupled.

The following must be considered according to prTS 50701 [15]:

1. Protection of safety functions
   Security threats should be prevented from exploiting vulnerabilities in control systems that would compromise the integrity of safety functions.
2. Compatibility of security countermeasures with safety functions
   The application of security countermeasures should not interfere with or reduce the integrity of safety functions.
3. Compatibility of safety function with security countermeasures
   The implementation and maintenance of safety functions should not compromise the effectiveness of applied security countermeasures.
4. Synchronization of safety and security activities
   Compatibility between safety functions and security countermeasures should be established, documented, validated, and maintained over the life cycle of the railway system from concept to decommissioning and removal.
5. Human dependability impact on safety and security
   Susceptibility of humans in the loop should be included in assessment of security vulnerabilities and their impact on the safety of system operation and maintenance.

4.2.3 Security Impact on Availability and Integrity

Integrity or availability problems in single parts of the CCS onboard system may still have significant impact on the effectiveness and usefulness of the whole system. In most cases integrity or availability problems will force the system to work, at least partially, in degraded mode to maintain safety. This again will have considerable impact on the availability of the system overall and on the ability to make use of the available physical infrastructure (tracks) and will render it near to impossible to increase the use of the physical infrastructure or to use the available physical infrastructure to its maximum capacity.

This would endanger one of the primary goals of the whole program, which aims at optimizing the use of the existing physical rail infrastructure to its maximum safe capacity. Failing to maintain integrity throughout the whole system will impact the ability to implement automated operation for large parts of the system thus endangering another goal of OCORA. The following direct impact factors of security on safety exist:

- Guaranteed Integrity of components, data and communication is a mandatory base for detecting safe states and decisions. If these signals cannot be trusted, safety decisions are based on "fake" information and do even not know if they are fake or not. If a man in the middle shows another state than the physical one is, the safety decision cannot be trusted.

If components are not available, safety cannot play its role and failsafe states will stop the resources and availability of the railway system. Availability can be compromised by DDOS-Attacks, malicious manipulations on physical and electronic level, through manipulated results of sensors that can hence no more be trusted.

4.2.4 Consequences

4.2.4.1 General

It is of vital importance that nowadays security measures are needed in order that safety can be trusted and develop its effectiveness. While for a commercial E-Order Portal most Client-Server connection nowadays use established secure and integrity-guaranteed communication protocols, safety needs at least this level and even more since lives of passengers rely on it. Three factors that must be considered, to profit from established safety frameworks when using nowadays digital technologies.

- By following existing rules and standards (application of codes of practice)
- By explicit risk analysis, where risk is assessed explicitly and shown to be acceptable.

The following subchapters detail each of these points:

4.2.4.2 Following existing rules and standards

A code of practice that is approved in other areas of technology and provides a sufficient level of IT security can be adapted to railways. This ensures a sufficient level of base security for safety. As a base for this work, the IEC 62443 [16] has been selected, as this standard series seemed to provide the best fit. With this approach, a normative base can be developed, based on IEC 62443 [16], and tailored for railways. It considers railway-specific threats and scenarios and yielding a set of IT security requirements. Assessment and certification of such a system can be carried out by independent expert organizations. IEC 62443 [16] addresses four different aspects or levels of IT security:

- general aspects such as concepts, terminology, and metrics: IEC 62443-1-x
- IT security management: IEC 62443-2-x
- system level: IEC 62443-3-x
- component level: IEC 62443-4-x

An information security management system (ISMS) shall be established for operation of the system. The aim of an ISMS is to continuously control, monitor, maintain and, wherever necessary, improve IT security. In the case of the ISMS, IEC 62443 [16] is based on the general stipulations of the ISO/IEC 17799 [20] and ISO/IEC 27000 [19] series.

The system and its architecture are divided into zones and conduits. The same IT security requirements apply within each zone. Every object, e.g., hardware, software, or operator (e.g., administrator) shall be assigned to precisely one zone and all connections of a zone shall be identified. A zone can be defined both logically and physically. This approach matches the previous approach for railway signalling systems very well. It has been used as the basis in numerous applications**.**

In IEC 62443 [16], the IT security requirements are grouped into seven fundamental requirements:

Requirements	Fundamental requirement (Area)
a)	identification and authentication control (IAC)
b)	use control (UC)
c)	system integrity (SI)
d)	data confidentiality (DC)
e)	restricted data flow (RDF)
f)	timely response to events (TRE)
g)	resource availability (RA)

Table 3 IT-Security requirements

In this standard, four security levels are distinguished. They are based on attacker types that the solution shall be protected against:

Security Level	Protection against attacker type
SL1	Protection against casual or coincidental violation
SL2	Protection against intentional violation using simple means with few resources, generic skills, and a low degree of motivation
SL3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and a moderate degree of motivation
SL4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and a high degree of motivation

Table 4 Security Levels

4.2.4.3 Explicit risk analysis

The risk analysis according to the OCORA (Cyber-) Security – Guideline [10], must be done by a team that has broad experience and knowledge. The result will be measures to have all risks in an acceptable area from the risk matrix. It shall be redone and especially mapped to technical risks, that can be influenced by technical measures. These measures must be taken over by the requirements and the architectural concepts.

4.3 RAM and Security

Another domain which also needs to be considered during the development of security solutions is RAM (reliability availability and maintainability). Specific availability targets can only be met if each system can operate uninterrupted in a secured environment with no influences from attacks like a DoS-attack (denial of service). Also, security processes like authentication of personnel and/or devices or like logging should not influence the availability for operations or maintenance. What is also important to be considered is that Integrity as a security goal influences availability through safety decisions, so if information from a safety relevant element misses reliable integrity, a failsafe decision will lead to unavailability.

5 Policy and Strategy for achieving Security

5.1 Security Protection Goals

Railway operators pursues a unified approach to securing information and information processing systems. The objective of security is to protect installations and systems on vehicles that use or contain ICT (Information and Communication Technology) against improper interference.

Security is not only protection against attacks from the outside world, but also against attacks from the inside and includes prevention of unwanted manipulation. The need for protection and the risk situation characterizes the requirements, which are continuously updated.

Due to the increased merging of IT and classic operations technology (train control, etc.) and the interconnection of all relevant components, security in general and as an enabler of safety is becoming increasingly important. Thus, the two disciplines, security, and safety, must be considered in their interdependence.

The definition of the security protection goals needs to be based on the specifications of the national authority for transportation (BAV, BMK, EBA, BMVIT, etc.), in particular the requirements for protection against unauthorized access and availability and the standard of the Federal Office for National Economic Supply, i.e. the standards IEC 62443 [16] and prTS 50701 [15].

The primary objectives of security are to ensure that security incidents do not result in safety incidents and to protect from cyber blackmail. In addition, security must support the reliable operation of a railway operator, in particular high availability, and integrity or, in the event of damage, i.e. "graceful degradation", while maintaining financial viability. Graceful degradation is a stability- and security-oriented reaction of a system to errors, unexpected events, or partial failures, in which the system maintains operation as good as possible.

The security protection goals are framed by generally accepted security objectives:

- Availability: The information and information systems are available within the planned thresholds.
- Integrity: The information is complete, up-to-date and is processed and transmitted as defined.
- Confidentiality: The information is only accessible to authorized persons/systems.
- Authenticity: The processing of information can be assigned to an instance or a person

Additionally, the general project objectives are structured in five objectives, each one contains an objective from the point of view of the railway operator and from the point of view of the customer.

The main objectives are:

- Safety
- Cost
- Capacity
- Availability
- Service Quality

Based on this, the following security protection goals are defined:

5.1.1 No "Safety" Incidents

In the area of railway infrastructure security is primarily dedicated towards securing the people from the system. Security must support this effort.

5.1.2 ISMS and Controls

Use processes and an ISMS (information security management system) according to ISO/IEC 27001 [19]. Use the controls of IEC 62443-3-3 [16]. Operate processes and an ISMS and strive for conformity with the standards ISO/IEC 27001 [19] and pr TS 50701 [15] (IEC 62443 [16]).

5.1.3 Financial Viability

Any security means shall be tested against the financial viability for the railway operator. It is counterproductive to define requirements, that are dropped in the procurement process caused by high cost.

5.1.4 Prevent Blackmail

Securing against cyber attacks of the attacker type "nation states" goes beyond the financial abilities of the railway operators. Therefore, this is not a goal. The current attack landscape shows highest activity and therefor probability for attacks driven by financial blackmailing.

5.1.5 Train Delay

The maximum tolerable delay caused by security incidents within railway operation needs to be defined and tracked (e.g., 100'000 minutes delay per year).

5.1.6 Maximal Total Failure Tolerance

The maximum tolerance for total failure caused by security incidents needs to be defined by each railway operator (e.g., one hour, within one hour a total service failure must be reinstated to a partial service level).

5.1.7 Maximal Partial Operation Tolerance

The maximum tolerance for partial operation caused by security incidents needs to be defined by each railway operator (e.g., four hours, within four hours a reduced service level must be reinstated to a normal service level).

5.2 Security Principles

Security is a collaborative continuous effort. All members including employees and partners are responsible for the protection of information systems and information in their area of responsibility, influence, and control.

The following principles are taken into consideration for OCORA. They shall support the achieving the ambitious security protection goals stated in chapter 5.1.The OCORA security principles represent a mind-set that underpins and influences the design and architecture of OCORA. They are the foundation for more detailed security related requirements that must be translated into functionalities by the suppliers.

The OCORA security principles have been derived from security standards and best practices to provide guidance for designing and architecting the complex system of an onboard CCS system. They are based on well-known security standards and best practices (i.e. ISO2700x [18], [19], NIST [17] Cybersecurity Framework [17], IEC 62443 [16]) as well as rail specific standards and best practices (i.e. prTS 50701 [15], EN 50126 [11]).

5.2.1 Secure by Design

Make security part of requirements, and not an afterthought. Protect a business application or information system against attacks by considering security requirements as part of its overall requirements.

- Experience has shown it is both costly and difficult to implement security measures after a system has been developed
- Avoid unnecessary development efforts by considering security requirements early on
- As security interferes with safety (e.g., timings, fail behavior) there must be a holistic approach

Implications:

- Understand the resulting security requirements in the engineering, design, implementation, and disposal of the system
- Security should treat the root cause of a problem, not its symptom

5.2.2 Defence in Depth

Avoid reliance on a single type of security control. Implementing security on multiple layers is better than relying on a single defence layer. If one security control fails or is bypassed, an additional layer can help preventing the attack.

- Identify and secure the weakest links first
- Use multiple security layers to increases the effort required for an attacker to compromise a system or application

Implications:

- Create a security architecture that documents the different layers of protection
- Balance defense in depth against simplicity and business needs
- Each subsequent security layer should not trust the previous layers
- Compartmentalize the system by defining security boundaries for information flows
- Prepare for the worst possible compromise scenario

5.2.3 Detectability (Logging & Monitoring)

It is impossible to manage something what you can not see nor measure. Exceptions, failures, and maybe outages will happen in complex systems, and these cannot be predicted with accuracy. Effective and continuous monitoring of system states is the key to detect deviations, failures, and attacks easily and early and to act swiftly to combat cascading failures or risks.

Implication:

- Start the logging & monitoring design with the goal of being able to detect breaches and compromise.
- Design components and systems to be able to log exceptions, vital heath and security events in a standard format and way

Design systems for secure and centralized logging (protection of log data in motion and at rest).

5.2.4 Design for Security Automation

Complexity can be managed easier when security related processes are automated. Manual security tasks are inefficient, expensive, and prone to inconsistencies and human error. It is no longer possible to deploy, operate, and secure complex applications and infrastructures without automation. Security, agility, scalability, and control are a direct function of automation in today's complex and rapidly changing technology and threat environment.

Implications:

- Automation reduces complexity and ensures consistency
- Reduces the talent gap by freeing scarce expertise form mundane tasks
- Automated testing
- Requires discipline and design

5.2.5 Secure by Default

Set secure default options to limit inherent security vulnerabilities. System or application configurations should favour security over not being secure. The default setting for a security control should be to deny access to a resource and require a configuration to specifically grant access. When the system goes into an error or exception state, these states must favour security over not being secure.

Implication:

- Security should not require extensive configuration and should just work reliably
- Establish secure defaults when system starts or goes in error or exception states
- Providing least privilege or making only necessary services and features available
- Use encryption by default for both data at rest and in transit

5.2.6 Simplicity over Complexity

Complexity is the worst enemy of security. Complexity in systems leads to increased human confusion, errors, vulnerabilities, automation failures, and difficulty of recovering from an issue. Favour simple and consistent architectures, designs, and implementations. Avoid unnecessary complexity. The more complex the system is, the more likely it may possess exploitable flaws.

Implication:

- Simplicity should be a key objective in design of systems and security
- Do not repeat yourself
- Reduce the variety and types of hardware and software
- Design systems that use the least resources possible (in terms of hardware and software)
- Favor convention over configuration
- Do not implement unnecessary security mechanisms
- Complexity makes vulnerabilities harder for developers and testers to uncover. Each feature, function, and interaction are a potential threat vector
- Complexity makes vulnerabilities harder to fix

Notes:

- No over-simplifying
- Balance reduced complexity against diversity required to achieve resiliency and reduced single-point-of-failures

5.2.7 Assume Failure & Compromise

Complex distributed systems lead to unpredictability and cascading failures. Even when all the individual components of complex system are functioning properly, the interactions between those components can cause unpredictable outcomes and vulnerabilities. Rare or surprising combinations of events, vulnerabilities, and creative user interactions make such systems inherently chaotic. In such systems prediction, complete testing, and modelling of all states is not possible in such systems with manageable efforts. Therefore, we must assume and account for failures and compromise.

Implications:

- Our systems are too complex to anticipate all potential interactions or vulnerabilities
- Assume that critical parts of the infrastructure are already compromised when designing architectures, systems, and components
- Embrace principles of chaos engineering and testing - facilitate real and repeated tests to uncover systemic weaknesses
- Design system for automated testability
- Establish continued and comprehensive monitoring of vital parameters to determine system health and security

5.2.8 Fail Safe and Secure (Graceful Degradation)

Failures should lead to a safe and secure state. Risk does not hurt - the impact does. If a security control fails, it should maintain a state of deny access. Design security mechanisms so that a failure will follow the same execution path as disallowing the operation. Prevent unauthorized access in case of errors, failures, exceptions, system degradation, or compromise**.**

Implication:

- Design to minimize the impact of component or control failures or compromise
- Confidentiality and integrity assurance top availability assurance
- Security methods (like authorized, authenticated and validated) should all return false if there is an exception during processing
- Assume system failure & compromise in design decisions
- Ensure safe reaction on denial

Examples:

- Dead man's switch is automatically operated if the human operator becomes incapacitated
- Traffic light controllers use a Conflict Monitor Unit to detect faults or conflicting signals and switch an intersection to an all-flashing error signal, rather than displaying potentially dangerous conflicting signals.

5.2.9 Usability & Manageability

Balance of security and usability - make secure behaviour easy instead of complex. Make it easy to do the right thing, make it difficult to do the wrong thing, and make it almost impossible to do the catastrophic thing. Security controls should not obstruct users in performing their work and should not be difficult to manage. User interfaces must be easy to use, so that users routinely and automatically apply the mechanisms correctly. This relates to the paradigm of Least Astonishment in UI design and Simplicity Principles

Implications:

- A component or system should be designed to behave in a manner consistent with how users of that component are likely to expect it to behave
- Design security interfaces and functions for ease of use, so that users routinely and automatically apply the protection mechanisms correctly

Note:

- If security gets in the way, sensible, well-meaning, dedicated people develop hacks and workarounds that defeat the security

5.2.10 Open Design

The security of a mechanism should not depend on the secrecy of the details of its design or implementation. Assume outsiders and attackers will have access to source code (also for closed source software) and complete design and network topologies. Assume sensitive information regarding security measurements are leaked or sold. Encourage proactive reporting of security issues or vulnerabilities and act on such reports.

Implications:

- Never store secrets in code, documentation, or configurations
- Open security design promotes faster improvement cycles
- Security measurements should be open and transparent

Examples:

- Shannon's Maxim: The attacker knows the system

5.2.11 Zero Trust

Assume everything to be insecure until a level of trust is established. The historic concept of trust that is based on a perimeter separating the inside from the outside does no longer hold in today's rapidly changing environment. Assuming no trust is a security model that more effectively adapts to the complexity of the modern environment. It embraces the mobile workforce, and protects people, devices, apps, and data wherever they are located.

Implication:

- Trust is not granted until the user, system, or component can be authenticated and authorized first
- Verify anything and everything trying to connect to a system before granting access
- Workforce: Authenticate users and continuously monitor and govern their access and privileges
- Workloads: Enforce controls across the entire application stack, especially connections between containers or hypervisors in the public cloud
- Data: Secure and manage data, categorize, and develop data classification schema, and encrypt data at rest and in transit
- Supply Chain: Question and assess the integrity and security of suppliers and the delivered products, systems, and services

5.2.12 Least Privilege

Only grant the minimal set of permissions that are necessary for a given action - and no more. Systems and users should operate while invoking as few privileges as possible. Granting permissions beyond the scope of the necessary rights of an action can allow a user or system to obtain or change information in unwanted ways. This principle limits the damage that can result from an attack, accident, or error. It also reduces the number of potential interactions among privileged systems to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur.

Implication:

- Minimize the system elements to be trusted
- This principle restricts how privileges are granted and revoked and timed out

5.2.13 Design Security for Safety

An insecure system is not safe (also called "security4safety"). This ensures that security threats are prevented from exploiting vulnerabilities in control systems that would compromise the integrity of safety functions. In addition, security functions and safety functions are separated so that security updates do not require safety recertification (separation of concerns). The security design of a system with safety relevance (SIL1-4) shall include the following means by level:

Implication:

- "Secure by design"
- "Defense in depth"
- "Detectability"
- System theoretic process analysis (STPA) for security with the concern's "safety", "crisis mode" and "availability".
- Ensure "heterogenity4security" (where possible, reuse dissimilarity)
- Separate the concerns of security and safety where possible
- Ensure a patch process inside the safety realm is available
- Make sure the system "fails safe" even when compromised.

Considering a security compromise or breach is caught through means on the respective level:

- The lower the risk is, the lower the number of the upper means is.
- The "difficulty of means" (and most likely cost) is higher, the higher the number of the upper means is.

5.2.14 Design Security for Innovation

Security shall be designed with innovation and agile development in mind (also called "security4agility"). Security functions are relevant quality attributes for the system.

Implication:

- Security means shall be made in a way, that agile development and innovation is still possible.

5.2.15 Design Legacy System Inclusion

Means for the secure operation of old systems are provided. New Systems and components will be introduced step by step over a timespan of at least 20 years. In that time those systems must cooperate with old systems with less security. Even after a complete deployment of completely new systems there will be systems interacting without the respective security means.

Implication:

- It must be possible to integrate legacy systems (e.g., locomotives) into new components and systems.
- Security must provide measures to handle such exceptions in a more secure way ("broken security").

Methods and technics for the integration of legacy systems encompass hardening, monitoring, ensuring least privileges are offered and compensating controls (technical, procedural) to name a few.

5.2.16 Heterogeneity for Security

Ensure availability even when full stacks must be shut down for security reasons. The system and components must be able to function even after massive security compromises have been detected.

Implication:

- If a major security weakness (systematic failure) is detected in an application stack (e.g. in APS), it must be possible to shut down that stack completely and run the corresponding region on a dissimilar other stack until the weak stack is patched, tested and put back into operation.
- Availability and dissimilarity shall be guaranteed for several weeks on a reduced (n minus 1) stack.

5.3 Security Guidelines

The security implementation guidelines provide further details on how the security principles will be applied.

The following are the implementation security guidelines:

- Dynamic Security
- Demand and promote security to suppliers
- Industrial collaboration
- Supply chain security
- Support Standardisation
- Build on available efforts from the partner railways
- Advanced availability and robustness
- Accountable operation and SIEM capability

5.3.1 Dynamic Security

Dynamic security via integrated toolchains in the Cyber Defence Center (CDC) up to the patching of the systems. Information about assets, security analysis, threats, and the risk assessment (impact, easiness, detectability) shall be combined with a dynamic feed of new vulnerabilities. The result is a real-time risk dashboard that shows where security actions/measures are most important.

5.3.2 Demand and Promote

Dialogue procedures with suppliers shall be used to determine what is affordable to maintain. The work in the standardization organizations is also essential about security and industry partners (EULYNX, RCA, etc). In this context, the following principles must be considered:

- Nation wide: use generic applications
- Europe wide - European Union Agency for Railways (ERA): use generic standards
- Industry - internationally: use generic products

5.3.3 Industrial Collaboration

Furthermore, a regular exchange with the various stakeholders needs to be maintained. The OCORA cooperation partners work closely together, whereby resources from the OCORA members are directly involved in the daily work.

5.3.4 Supply Chain Security

It must be ensured that the complete supply chain (suppliers, contractors, vendors, and operators) is understood and supports all security efforts (like cybersecurity verification, cybersecurity validation and cybersecurity assurance).

5.3.5 Support Standardization

All railway operators shall support standardization projects of security in Europe (example: RCA; EULYNX Baseline 4; prTS 50701 [15]; FRMCS).

5.3.6 Build on available Efforts

Build on available efforts of the partner railways. Close coordination with cyber security departments from railway operators and other partners shall be maintained.

5.3.7 Advanced Availability and Robustness

The solution offers continuous operation and availability even if faced with partial failures (controlled graceful degradation). It has no single point of failure in elements that cause domino effects or have high leverage in terms of availability. Any loss of integrity or failure must be revealed instantaneously. The system will actively prevent triggering safety reactions.

5.3.8 Accountable Operation and SIEM Capability

The solution (-process) must provide real-time security related monitoring including all operational interventions such as trouble shooting, deployment, configuration management and change management. All participating elements have a properly authenticated identity. No anonymous components are accepted.

6 Preliminary Analysis of Security Implications

The whole system has grown in time and in technology. It is a patchwork with spreading of many elements over the whole country and with interfaces and relations to neighbouring countries. The high number of interfaces and interdependencies pose a high risk for cross company infections and incidents. Old analogue systems, electronic interlocking and digital control are all existing beside each other. Since security always depends on the weakest element in the chain, the vulnerabilities are manifold. With the actual strongly increased cyber vector for attacks and the simple possibilities in organizing vandalism over social channels, the rail system has become very vulnerable to intentionally motivated attacks. The following table gives an overview about today´s security.

Security topic	Statement	Rating
Architecture and Zoning Segmentation and Isolation	The security level on currently used train have too low security levels, which was shown in Audits. These audits revealed that almost no or only a few architectural concepts existing. No network separation.	poor
Physical Security	Very low security on parked vehicles. Technical Systems can be easily manipulated, even when the vehicles are locked. A person could access and activate a train with only few tools. The sidings, platforms and other areas with easy access bear critical network and access to network elements.	very poor
Identity a. Access Management	Low or no IAM	very poor
Authentication	Low or no authentication	very poor
Authorisation, Role models, Access Control	Poor or not existing authorization, except for ETCS.	very poor
Integrity assurance, Checksums in transit and at rest.	Safety mechanisms are in place, but manipulation is possible due to poor physical security and often not applied security mechanisms.	poor
Non-Repudiation, Logging	Manipulation cannot be detected properly. The consequences on operational side are only discovered when safety is directly involved.	very poor
Confidentiality of data at rest	The requirements of the applications are very low. To prevent attacks, the chain for cyber-attacks including fingerprinting before attacking the confidentiality must be raised. However, to prevent attacks, the entire attack chain for cyber-attacks including fingerprinting prior to the attack on confidentiality must be increased.	poor
Confidentiality of data in transit	On modern trains confidentiality is very low. Confidentiality within on-board networks is very low. The use of industrial protocols and technologies does not always allow implement security. External communication is not always cyphered.	very poor
Security Monitoring, SIEM, SoC	Application monitoring only exists on newer trains. Security related monitoring does often not exist.	poor
Availability, Business Continuity Backup/Restore	Average level on newer trains. Few redundancies and fallback possibilities are available.	poor
Resilience against actual advanced attacks	Poor level due to almost inexistent security application of good and best practice. Topic is being addressed presently with manufacturers. Running trains are not sufficiently secured and can easily be manipulated. So, operational disruptions and even accidents can be provoked.	very poor

Table 5 Security topics at railway systems

6.1 Results of the analyse from today's Security

6.1.1 Architectural deficits on trains

Trains are nowadays rolling datacentres. Datacentres need a high level of architectural protection measures. On trains we have today only very few segregations of networks and services. The co-existence of passenger services like Wi-Fi, public screens, passenger information and train control elements, pose a risk of hopping and lateral movement attacks. Not only targeted attacking but also electronic vandalism must be prevented from. Modern trains are much high exposed to it than older trains because of the increased attack vector of cyber and local attacks.

6.1.2 Physical security on trains

Another critical gap is the physical security of locomotives. Locomotives and train compositions are sometimes left unlocked. Apart from this, it is currently also possible to use the simplest means to gain unauthorized access to a driver's cabin. A state-of-the-art, future proof IAM concept, which ensures access even when the vehicle is disconnected, must be implemented

6.1.3 Interoperability of the trains

Another aspect that needs to be clarified at an international level is the interoperability of the trains. Even when crossing a border, it must be ensured that all essential security and safety functions are fully guaranteed.

6.1.4 Confidentiality of data on trains, missing basic communication confidentiality

Since old protocols are used even on new trains, communication can easily be listened to, analysed, manipulated, or interrupted. Even though the content is not a very confidential information itself, but the simple possibilities to analyse it and the poor integrity checks and controls pose a high risk of manipulation. When signals cannot be trusted, also safety functions with good concepts are worthless. The whole chain of attack starts always with information gathering. only confidentiality and cyphered information interrupts this attack vector from beginning. Here we have a gap that must be filled.

6.1.5 In general, poor security level in almost all disciplines on trains

Even old trains pose a quite high risk of weak protection against intentional attacks. It is easy to access a train cockpit and start driving.

Newer trains start to have some security measures against intentional misuse but have a much higher potential in cyber security and physical/technical combined attacks

A modern train is a rolling datacentre. In datacentres we apply high standards for security. On a train, they are low. It starts with broadly available information on the internet continues in very poor physical security and ends up in old technologies in communication, authentication, and access management. Intentional attacks could interrupt or damage safe operation significantly.

6.1.6 Low Resilience against advanced or targeted attacks

The train system has grown over time in size and technology. Long invest cycles pose the risk of always being too late with measures against actual attack scenarios. This is in general a problem. Digitalization can only happen if security is considered seriously. With OCORA a significant higher level for security must be reached in all areas from beginning. Only with that we can catch up with basics in security, while the threat landscape grows significantly. The long invest cycles will very soon drive us back again behind actual threats.

7 Planning of Security Activities

The main targets of the OCORA security workstream are the following:

- Creation of a cyber security engineering process (with risk management)
- Integration of (cyber-) security thoughts like zoning and security principles for the OCORA architecture
- Security documentation (Guideline, Concept, Project Cybersecurity Management Plan)
- (Cyber-) Security Requirements specification (CRS) on system and subsystem level

Chapter 3 has shown how important security solutions are for railway operators, therefore OCORA is required to consider security aspects of CCS on-board solutions as well.

As mentioned in the Introduction to OCORA-BWS03-010 – Introduction to OCORA [7] (cyber-) security is one of the main design goals (modularity, interoperability, replaceability, modifiability, adaptability, **security,** and usability) this includes:

- Creation of a security process (including security risk management) to achieve a well-founded security concept and requirements (see OCORA-TWS06-020 – (Cyber-) Security – Guideline [10]).
- Ensure that the security requirements are short formulated (e.g., through pointing to existing standards and security/maturity levels where possible).

For information about the organizational structure, scope, main targets, and deliveries from OCORA please refer to the document OCORA-BWS03-010 – Introduction to OCORA [7].

7.1 High Level Documentation Overview

The current strategy to cover the cybersecurity documentation for OCORA is shown in Figure 7.

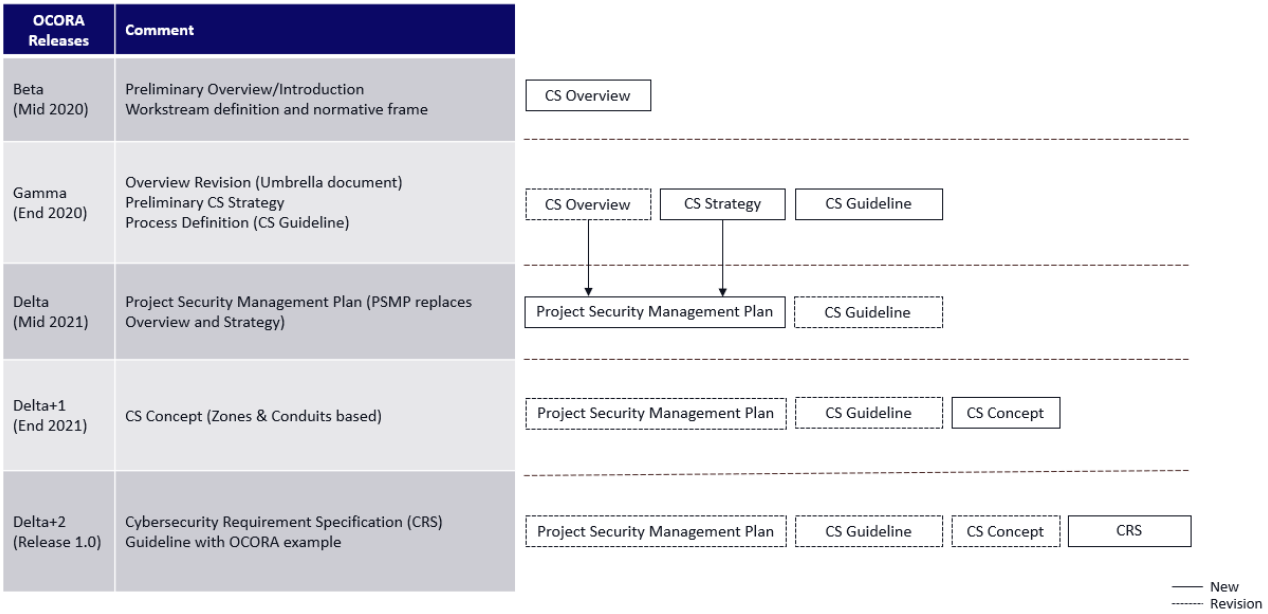

Figure 7 Security document structure and timeline

7.1.1 CS Overview

A predecessor to this document, captured the introduction of security for OCORA and defined a frame in terms of applicable standards and interfaces. This document is risen and has evolved to the Project Cybersecurity Management Plan.

7.1.2 CS Strategy

A predecessor to this document, gave a general look at security strategies. Please see chapter 5 for the strategy of the OCORA project.

7.1.3 CS Guideline

This Document gives a deep look and walkthrough of the security process. Please refer to the document OCORA-TWS06-020 – (Cyber-) Security – Guideline [10].

7.1.4 Project Cybersecurity Management Plan

This document.

7.1.5 CS Concept

The OCORA security concept will be available after all security tasks (defined in the OCORA-TWS06-020 – (Cyber-) Security – Guideline [10]) are completely carried out. It will be released with the OCORA Release Delta+1 in 2021.

7.1.6 Cybersecurity Requirements Specification

The goal of the Cybersecurity workstream is the Cybersecurity Requirement Specification (CRS). In phase 4 according to EN 50126-1 [11] on system level and in phase 5 on subsystem respectively component level. The figure below shows the cybersecurity assurance process according to prTS 50701 [15] including the CRS.

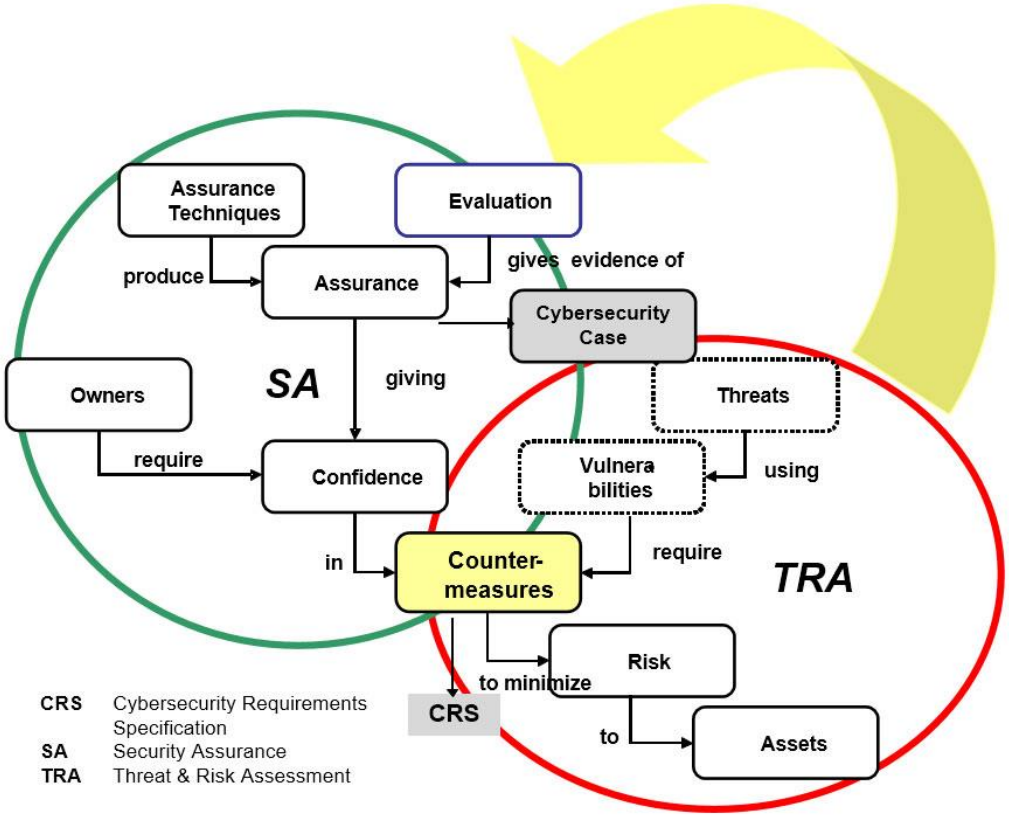

Figure 8 Cybersecurity Assurance Process according to prTS 50701

7.2 Cybersecurity Activities Management

7.2.1 Project Organization

The basic project organization is defined in the OCORA-BWS03-010 – Introduction to OCORA [5] and in OCORA-TWS01-100 – CENELEC Phase 1 – Concept [21]. The detailed project organization chart will be available in the phase 2 document Project Management Plan (PMP) according to EN 50126-1 [11].

7.2.2 Role and responsibilities

Actors, roles, and stakeholders with responsibilities are defined in the OCORA-BWS01-020 – Glossary [2].

7.2.3 Interface with other stakeholders

The Cybersecurity workstream includes collaboration with other work groups.

Topics interfacing with other work groups:

- Compatibility with European NIS Directive, RCA and EULYNX
- Integrate the results of the TOBA project / FRMCS initiatives
- Integrate the results of the Shift2Rail program (X2rail1 and X2rail2)
- Contribution of ER-ISAC

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

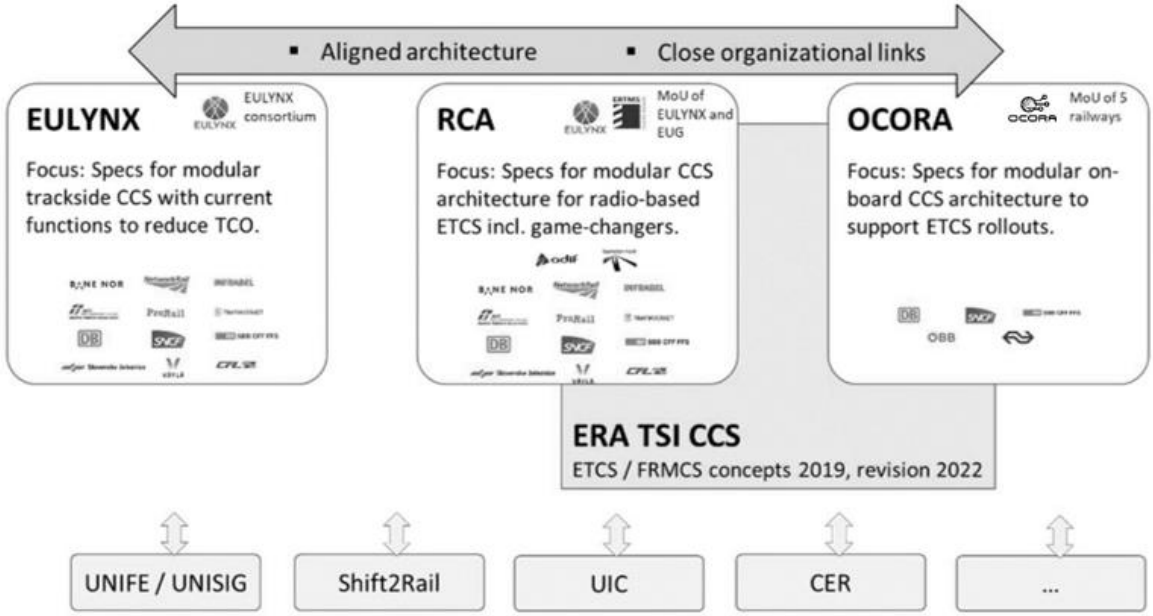

Figure 9 Relations of EULYNX, RCA and OCORA[4]

More information is available in OCORA-BWS03-010 – Introduction to OCORA [5].

7.2.4 Key Milestones

Key milestones are presented and developed in consecutive releases (Alpha, Beta, Gamma, etc.). Detailed information is present in OCORA-BWS05-010-Delta – Road Map [22] and described in OCORA-BWS03-010 – Introduction to OCORA [5]

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

7.3 Security Engineering Process

7.3.1 Introduction

The EN 50126 [11] 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 [11], to apply the security engineering processes proven in other industries, e.g. IEC 62443 [16]. The upcoming standard EN 50701 [16], currently as prTS 50701 [15], 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 [11]. 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 [11] 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. 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.)

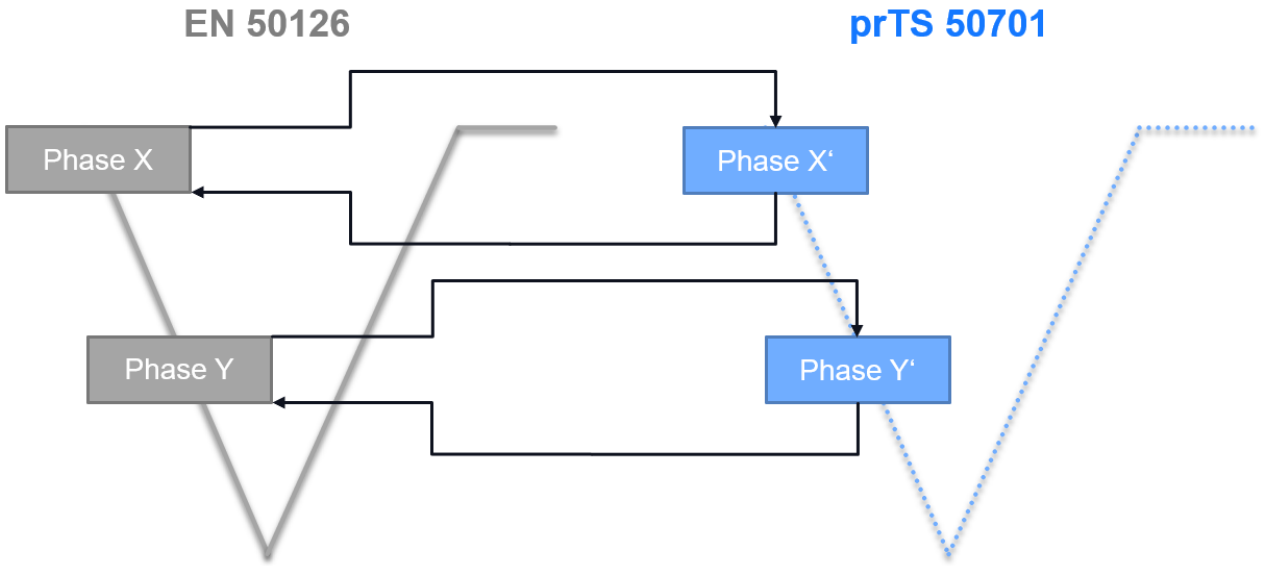

Figure 10 Process Interaction

Security solutions are not subject to assessment in contrast to railway solutions, which are developed according to EN 50126 [11]. 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 [11] 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 [15]. The result of each phase on the security side must be verified. This is a cyber security verification activity, which is not related to any safety guidelines or standards. This lays the base for the validation and cyber security system acceptance.

The phases of the security engineering process should be mapped to the equivalent CENELEC phases to ensure the verification- and/or validation tasks are also performed for the results and outputs from this process. It is up to the railway operator to implement this mapping. The responsibility of integration of the security solution lies also with the railway operator. In addition to a secure operator concept, a secure solution also includes a secure system integration and secure solution implementation according to IEC 62443 [16] and

prTS 50701 [15]. 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.

	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 Initial Risk Assessment	Zone based detailed 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 6 Mapping Security Model to EN 50126 Phase Model (phase 1-5)

The security activities are organized within the nine streams shown in Figure 11. These streams are described in the chapters 7.4 - 7.9 in more detail. These chapters have the focus on the CENELEC phases 1-5 according to prTS 50701 [15]. Nevertheless, further considerations for the CENELEC phases 6-11 are presented in chapter 8.

Stream	Goal
Ensuring appropriate degree of personnel independence	Proper governance / segregation of duties for staffing of roles.
Maintenance of security related documentation	Documentation and understanding of system under consideration is always up to date and consistent.
System design	Cyber security related aspects are taken in account in the system design.
Risk management	Cyber security risks are properly analyzed (with respect to RAMS) and mitigated.
Identification, coordination and resolution of conflicts	Possible conflicts between cyber security and RAMS / functional requirements of the SuC are identified, resolved and documented.
Definition of process for infrastructure for testing and integration	Aspects of integration and testing are considered at early enough stages of the lifecycle.
Verification	CENELEC-requirements of each lifecycle phase have been fulfilled.
Validation	Cyber security requirements have been properly specified and system has been implemented according to these requirements.
Analysing of maintenance, performance and operation	The system remains secure also in late stages of the lifecycle after the project phase is over.

Figure 11 Workstream activities

7.3.2 Process Evaluation

A process evaluation is presented in the document “OCORA-TWS06-020 – (Cyber-) Security – Guideline” [10].

7.3.3 Security Risk Assessment Structure

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

- Architectural Design with Zone Concept
- Threat Analysis
- Risk Analysis (structural analysis)
- Measures
- Integration / Security Architecture / Specification

7.3.4 Security Risk Assessment Approach

There are two approaches to define the security measures based on a risk analysis. Following the standards, NIST 800 [17], IEC 62443 [16], ISO 27005 [18] 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 [11] / 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 [11]) - no basis for continuous improvement process

Table 7 Advantages and disadvantages of static and functional approaches

After evaluating Table 7, 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.

A detailed description of the OCORA-V-cycle can be found in OCORA-BWS08-010 – High Level Methodology [8]. It provides information about the following aspects and how they are defined:

- General Process
- CENELEC Phases
- Deliverables from the OCORA work group
- Review process
- Verification & Validation

7.4 Ensuring appropriate Degree of personal Independence

Personnel independence in the review process can be ensured by our OCORA security organization. The security managers from the projects give their documents to the security managers of OCORA who conduct the review.

Goals	**Appropriate degree of personnel independence for tasks that require such independence.**
Phase	1-12
Inputs	-
Activities	Verify that verification tasks are carried out by the defined, responsible role and that role was not involved in the creation of the artefact under scrutiny. The same principles as for the RAMS activities are applied. (c.f. RAM or Safety-Plan).
Outputs	Documentation of verification in the verification report of each phase.

Table 8 Personal independence

7.5 Security related Documentation

Phase	**Activity**
1	Complete PSMP (this document)

Table 9 Security documentation

7.6 System Design

Phase	**Activity**
2	Identify assets for essential functions Review logical and physical network plans Apportionment to zones and conduits
3	Verify and leverage possibilities to optimize security by design
4	Refine normative requirements to SuC specific requirements Specify requirements for secure disposal
5	Assign technical security requirements to components

Table 10 System Design

7.6.1 Identify assets for essential functions

Goals	**The necessary assets/components of the SuC that are necessary to realize the essential functions of the system are identified and documented.**
Phase	2
Inputs	Essential functions (capabilities) of SuC
Activities	Review the list of essential functions (capabilities) for the SuC and identify the assets/components that are necessary to realize those functions.
Outputs	List of essential functions and assets/components necessary to realize these functions in threat risk analysis.

Table 11 Identify assets for essential functions

7.6.2 Apportionment to zones and conduits

Goals	**Ensure that the SuC fits well into the overall zoning concept of OCORA, and the overall zoning construct remains manageable.**
Phase	2
Inputs	OCORA Zones and conduits concept System boundaries Initial system architecture, incl. list of functions, interfaces, and generic systems Logical and physical network plans Results of review of logical and physical network plans
Activities	Review the OCORA Zones and conduits concept and specify the zones where the SuC will be placed in as well as the conduits connecting these zones. Specify the data flows transferred through these conduits for each conduit. Whenever possible use existing zones and try to not add additional micro-segmentation (the overall zoning construct aims to remain manageable!) If additional zones are necessary, develop these zones in accordance (and in exchange) with RCA/EULYNX.
Outputs	System architecture including zones and conduits showing the positioning in the overall zoning concept of OCORA documented in threat risk analysis.

Table 12 Apportionment to zones and conduits

7.6.3 Verify and leverage possibilities to optimize security by design

Goals	**Ensure that potential to improve security by adapting the system design (security by design) do not go unnoticed and are discussed in accordance with other RAMS and functional requirements.**
Phase	3
Inputs	System boundaries Initial system architecture Results of impact analysis Results of high-level risk analysis (scenarios)
Activities	Review the system architecture regarding security risks identified in the impact and high-level risk analysis. Analyse and document possibilities to eliminate risks by adapting the system design. If possible and potential conflicts with RAMS or functional requirements can be resolved to everybody's benefit, adapt the system design.
Outputs	If necessary: Adaptions to system design

Table 13 Verify and leverage possibilities to optimize security by design

7.6.4 Refine normative requirements to SuC specific requirements

Goals	**Ensure the normative requirements are refined to be applicable to the SuC.**
Phase	4
Inputs	System architecture Results of high-level risk analysis (scenarios) (Intermediary) Results of detailed risk analysis (especially selection of normative IEC 62443 [16] security requirements). If available: Additional risk mitigation measures
Activities	During the risk analysis, security requirements will be selected in an iterative approach. Further risk mitigation requirements might be added during this process. These requirements need to be refined to be meaningful for the system under consideration. Once the requirements are refined (applicable and meaningful) for the SuC the output is passed back to the risk management process. (The complete picture of the interaction of risk management and system design is described in the chapter "risk management".)
Outputs	Zone based Cybersecurity Requirements Specification (CRS) (incl. application conditions) containing refined (applicable and meaningful) requirements for the SuC. See chapter 7.1.6.

Table 14 Refine normative requirements to SuC specific requirements

7.6.5 Specify Requirements for secure disposal and renewal

Goals	**Ensure the necessary thoughts and ideas for secure disposal and renewal of the system are developed early in the system lifecycle.**
Phase	4
Inputs	System architecture Functional requirements of the system
Activities	Review the system architecture and functional requirements of the SuC and analyse the implication for secure disposal and renewal. Formulate these ideas as requirements for secure disposal and renewal.
Outputs	Requirements for secure disposal and renewal in the CRS

Table 15 Specify Requirements for secure disposal and renewal

7.6.6 Assign technical security requirements to components

Goals	**Entering phase 5 the focus of the CENELEC process shifts from concepts to solutions. in this phase the system will be apportioned into several subsystems. For traceability and completeness of the implementation of Cyber Security System Requirements, a clear top-down perspective from high level system requirements to component and implementation level shall be adopted. Traceability of requirements through the different level of refinements is a prerequisite for verification activities. Ensure, the CRS defined in earlier stages is broken down to system components and gets implemented by specific security measures.**
Phase	5
Inputs	System architecture breakdown to components, incl. SuC inventory Cybersecurity Requirements Specification (CRS)
Activities	Analyse the Cybersecurity Requirements specified in the CRS and attribute each requirement to all components and subsystems of the SuC. Document the relationships between component compliance and requirements.
Outputs	Component based Cybersecurity Requirements Specification (CRS Breakdown) incl. application conditions.

Table 16 Assign technical security requirements to components

7.7 Risk Management

Phase	Activity
1	CIA-NPR analysis, classification, and categorization Challenges & approaches
2	Definition & update of threat landscape. Impact analysis for the SuC Definition of risk acceptance criteria and scaling of risk matrix
3	High-level, zone-based risk analysis Refinement of initial threat assessment in threat log
4	Detailed risk analysis Definition of organizational and physical requirements and/or application conditions
5	Component based risk analysis update and definition of compensating countermeasures

Table 17 Risk Management

The risk management activities are performed iteratively and are distributed over several CENELEC phases. See also the document “OCORA-TWS06-020 – (Cyber-) Security – Guideline” [10].

7.7.1 CIA-PNR analysis, classification, and categorization

Goals	The CIA-PNR properties of the SuC are understood and the system's categorization is documented.
Phase	1
Inputs	Purpose and scope Applicable security standards
Activities	Analyse CIA (Confidentiality, Integrity, Availability) - PNR (Privacy, Non-Repudiation, Retention) properties according to the purpose and scope of the SuC.
Outputs	CIA-PNR-Analysis and categorization

Table 18 CIA-PNR analysis, classification, and categorization

Classification according to CIA-PNR analysis:

The model joins the 3 areas of internal information security classification with the 3 areas of regulatory responsibilities. Any information within the project’s needs be reviewed and classified with the CIA-PNR scheme. With this model we can ensure to set up the right data handling and protection mechanism. The left side is the inside view of the property, e.g., Confidentiality → "I want to protect my data from access by someone else" and the right side the public and regulatory demand "We have to treat certain data secretly". The same applies to the other properties.

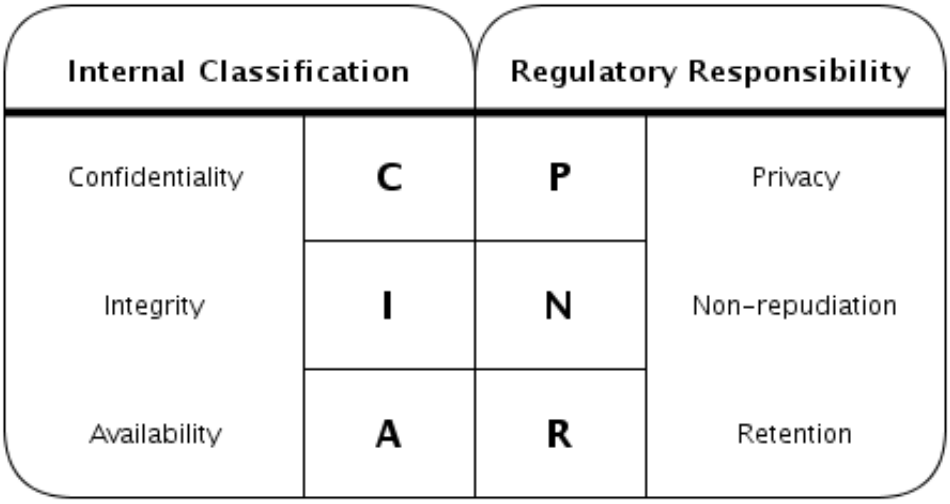

Figure 12 CIA-PNR classification

The classification scheme will always use the same three levels for all classification criteria:

Level	Meaning
0	No requirements at all. Therefore, no technical measures must be taken to full fill the requirements for the classification criterion.
1	Basic requirements. This level denotes the usual standard requirements for most business data and systems. In most cases standard measures and solution will fulfil the requirements. Standard infrastructure (systems) will be required to full fill requirements for this level.
2	Special requirements. Enhanced technical measures are required to address the requirements. On this classification level, the individual requirements must be explicitly described, and measures be defined that address these requirements.

Table 19 Classification Levels

7.7.2 Challenges & approaches

Goals	**Challenges and approaches to cyber security are analysed and documented on the same, very high level of abstraction, as the CIA analysis.**
Phase	1
Inputs	Purpose and scope Applicable security standards CIA-PNR-Analysis
Activities	Analyse challenges and approaches according to the purpose and scope of the SuC. Plan these activities in the PSMP (in this document).
Outputs	Challenges and approaches

Table 20 Challenges & approaches

7.7.3 Definition & update of threat landscape

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 threats that could jeopardize the railway transport system. Agreement on threat landscape is crucial as discrepancies in the set of considered threats by the different stakeholders will lead to risk underestimation and lack of control implementation. Hence, all stakeholders should to participate in a process to agree on a generally accepted threat landscape. The threat landscape should be based on recognized threat library/reports and built with a high-level approach providing an overview of the threats applicable to the railway sector.

Goals	Ensure the threat landscape for the SuC is defined, understood and up to date.
Phase	2
Inputs	Purpose and scope Initial system architecture Logical and physical network plans Essential functions
Activities	The threat landscape is a summary of available threat information such as threat sources, threat vectors and trends that may affect a defined target Consider the following high-level threats for applicable threats and enter them into the threat log: • Physical attacks • Unintentional damage and loss of information or IT assets • Outages • Eavesdropping, Interception and Hijacking • Intentional attacks / Abuse • Legal Non-Compliance • Scan the following libraries and reports for additional threats • ENISA Threat Landscape Yearly report • Provide a mapping of the threats to the input threat library/report • Provide rationale for not considered threats
Outputs	High level threats in scope, documented in the threat log

Table 21 Definition & update of threat landscape

7.7.4 Impact analysis for the SuC

Goals	Understand the high (top) level impacts of cyber security risks on the business.
Phase	2
Inputs	Purpose and scope Initial system architecture Logical and physical network plans Essential functions
Activities	Assess the impact and criticality of losing the component integrity, availability, or confidentiality for the SuC and its components if they are known. This impact evaluation shall measure the worst global impact in case of loss of the component considered properties. The global impact shall be evaluated not only at the business level, but also at the environmental and human impact levels. Document the assessment results. Consider at least the following impacts: • Disclosure of confidential data: Unauthorized parties gain access to internal, confidential, or secret information. Consequences are manifold and depend on the intention of the respective party. Disclosure of confidential data can also be the cause of other impacts below. • Noncompliance (regulatory requirements are unclear, so far, only net neutrality was considered): Regulations or laws are violated, leading to authorities demanding fines from or imposing operational restrictions from the OCORA members. • Reputational damage: Public perception of customers and partners is damaged, possibly leading to loss of revenue, jobs, confidence and/or public ridicule. • Safety risks for humans and environment: Death or injury of passengers, bystanders, or personnel. Destruction of rolling stock, infrastructure, or environment. Can also lead to reputational damage. • Disruption of the rail network or services operating on it: long- or short-term interruptions of small. or larger areas.
Outputs	Top level impacts documented in threat risk analysis

Table 22 Impact analysis for the SuC

7.7.5 Definition of risk acceptance criteria and scaling of risk matrix

Defined in the document “OCORA-TWS06-020 – (Cyber-) Security – Guideline” [10].

7.7.6 Refinement of initial impact assessment in threat log (scenarios)

Goals	**The top-level impacts are illustrated with several documented scenarios.**
Phase	3
Inputs	Purpose and scope Initial system architecture Logical and physical network plans Essential functions Impact analysis
Activities	Refine the identified impacts with scenarios, that describe how the impacts might come into existence. Document assumptions and conditions for the scenarios to come into reality.
Outputs	Scenarios documented in threat risk analysis.

Table 23 Refinement of initial impact assessment in threat log

7.7.7 High-level, zone-based risk analysis

Goals	**The risks per zone and conduit of the SuC are identified and analysed. Potential of architectural or conceptual changes for eliminating or reducing risk is identified and realized.**
Phase	3
Inputs	Threat log Threat landscape Impact analysis Impact-scenarios
Activities	Further refine the scenarios identified during impact analysis further per zone and conduit. Add the information identified according to the threat landscape and synthesize an encompassing threat log. Synchronize the resulting threat log with RAMS the hazard log. Analyse possibilities to reduce or eliminate risk by changing the overall architecture or overall concept of the SuC. Document the analysis including the decisions taken.
Outputs	Threat log; Log of considerations for eliminating risk by architectural / conceptual changes.

Table 24 High-level, zone-based risk analysis

7.7.8 Detailed risk analysis

See the document “OCORA-TWS06-020 – (Cyber-) Security – Guideline” [10].

7.7.9 Definition of organizational and physical requirements and/or application conditions

Goals	**Organizational and physical security requirements are identified and documented. Application conditions are identified and documented**
Phase	4
Inputs	Threat log Results from previous iterations
Activities	Review the threat log and define applicable organizational and physical countermeasures. Document assumptions on the system, it is environment and operation as application conditions.
Outputs	Updated threat log Cybersecurity Requirements Specification

Table 25 Definition of organizational and physical requirements and/or application conditions

7.7.10 Component based risk analysis update and definition of compensating countermeasures

Goals	**Ensure the traceability of risks identified for the SuC to its components after the breakdown into components. Additional necessary compensating countermeasures are identified.**
Phase	5
Inputs	System architecture breakdown to components, incl. SuC inventory Threat log
Activities	CENELEC phase 5 creates a system architecture breakdown to components, incl. SuC inventory. Based on this breakdown traceability of the cybersecurity requirements defined in the CRS (prior two activities) must be demonstrated. For each item in the CRS as well as each organizational/physical requirement and each application condition answer the following questions: • For what part of the SuC is this item relevant? How will it be implemented? • What is the contribution of the implementation in a part of the SuC to the overall security posture? Ensure that no CRS item goes without a match in the architectural breakdown.
Outputs	Cybersecurity Requirements Specification (CRS) breakdown

Table 26 Component based risk analysis update and compensating countermeasures

7.8 Identification, Coordination, and resolution of conflicts

Phase	Activity
1	Identify necessary contacts to analyse and resolve conflicts
2	Analyse top impacts for potential conflicts
3	Identify and document risks with potential implications in other fields
4-5	Identify, document, and resolve conflicting measures

Table 27 Identification, Coordination, and resolution of conflicts phase 1-5

7.8.1 Identify necessary contacts to analyse and resolve conflicts

Goals	**The contact people for RAMS, BCM as well as functional topics are identified and introduced to the SuC security manager.**
Phase	1
Inputs	Organigram, individual contacts/networks
Activities	Create a list of contacts/people that will need to be involved to analyse and resolve conflicts. As a security manager: Introduce yourself to the people on that list. Minimal requirements for this list: • at least 1 contact for RAM aspects • at least 1 contact for Safety aspects • at least 1 contact for BCM aspects (Business Continuity Management) • at least 1 contact for functional topics
Outputs	List of contacts to resolve conflicts

Table 28 Identify necessary contacts to analyse and resolve conflicts

7.8.2 Analyse top impacts for potential conflicts

Goals	**The top-level impacts identified in the risk management stream are validated and enriched with similar RAMS, BCM results.**
Phase	2
Inputs	Top level impacts Similar results from other areas
Activities	Analyse each impact for its implications in other areas, especially RAMS and BCM. What does this impact mean for these areas? Is the view in other areas the same? Are there additional impacts, that need to be considered?
Outputs	Results of impact/conflict analysis documented in threat risk analysis

Table 29 Analyse top impacts for potential conflicts

7.8.3 Identify and document risks with potential implications in other fields

Goals	**The implications of documented high level, zone-based risks are understood and documented.**
Phase	3
Inputs	Threat log (zone based) Hazard log (safety) and similar results from RAM and BCM
Activities	Analyse the zone-based risks for links of similar results (e.g., hazards in the hazard log) to other areas. Identify matching items in other results and analyse synergies in the mitigation strategies. Identify potential conflicts with items in other results. Standardize the wordings in the different logs and results, such that matching items carry the same names.
Outputs	Result of impact-analysis on other fields documented in threat log

Table 30 Identify and document risks with potential implications in other fields

7.9 Process and infrastructure for testing and integration

Phase	Activity
3	Specify testing infrastructure and procedures throughout the lifecycle
4,5	Specify testcases for each cybersecurity requirement

Table 31 Process and infrastructure for testing and integration

7.9.1 Specify testing infrastructure and procedures throughout the lifecycle

The minimal testing activities depend on the security category of the zone or sub-zone of the SuC.

Goals	The testing infrastructure and necessary procedures are documented.
Phase	3
Inputs	Categorization according to the project security management plan System designs Zones and conduits
Activities	Create test documentation including the necessary testing activities according to the security category of a system. Plan the different activities and control mechanisms in the test documentation. Minimal set of topics for test documentation: Test plan (Necessary infrastructure, data, and procedures for testing. Is testing done with live data? Copies of live data? On what infrastructure? And with what procedures? Definition of testing roles and responsibilities, define the necessary content of the Test Report, what testcase was tested when, by whom, on which infrastructure?) Measures for secure disposal and renewal Initialize activities to source contractors for tools, penetration tests and read teaming if necessary.
Outputs	Input for the Test documentation

Table 32 Specify testing infrastructure and procedures throughout the lifecycle

7.9.2 Specify testcases for each cybersecurity requirement

Goals	Enhanced quality of requirements specification Ensure that requirements are testable or at least rationally verifiable
Phase	4, 5
Inputs	Test concept Cybersecurity requirements specification (CRS - zone based in phase 4 and component based / breakdown in phase 5)
Activities	For each cybersecurity requirement: 1. Analyse the requirement and identify ways to verify its proper implementation 2. Define a test strategy for the requirement and document a test case, make sure the test result is measurable or at least verifiable
Outputs	Test specification for each requirement

Table 33 Specify testcases for each cybersecurity requirement

7.10 Verification

Phase	Activity
1-5	The verification step at the end of each phase verifies that all formal requirements of the CENELEC method are satisfied. This means, that all activities have been carried out according to the PSMP and all results have been documented in the way specified by the PSMP. Also for each activity a statement, whether the goal of the activity was reached must be documented by the verifier.

Table 34 Cybersecurity Verification phase 1-5

7.11 Validation

Phase	Activity
4	The phase 4 validation verifies the integrity of the documentation produced during phases 1 to 4. It also contains a judgement of the risk analysis and its conclusions and verifies the proper and complete specification of the cybersecurity requirements as well as organizational and physical countermeasures.

Table 35 Cybersecurity Validation phase 4

7.12 Maintenance, Performance and Operation

Phase	Activity
3	Consider business continuity aspects (incl. incidence response and recovery) for the SuC
4	Plan for security monitoring and vulnerability management
5	Assign responsibilities for organisational and physical requirements Establish third party management for security, including supplier security capabilities and support contracts

Table 36 Maintenance, Performance and Operation phase 3-5

7.12.1 Consider business continuity aspects (incl. incidence response and recovery) for the SuC

Goals	Ensure business continuity aspects are already considered at early lifecycle stages
Phase	3
Inputs	Logical and physical network plans and review Zones and conduits Essential functions (capabilities) Impact analysis results
Activities	Analyse the system for its implications in incident response. How can the essential functions be recovered as quickly as possible and what are the requirements to do so? Define BCM measures according to the above analysis. Compare and discuss the results of this analysis with BCM responsibilities in the organization.
Outputs	BCM analysis documented threat risk analysis

Table 37 Consider business continuity aspects for the SuC

7.12.2 Plan for security monitoring and vulnerability management

Goals	**Ensure that security monitoring and vulnerability management activities and capabilities are planned for in early lifecycle stage.**
Phase	4
Inputs	Logical and physical network plans and review Zones and conduits Essential functions (capabilities) Impact analysis results
Activities	Analyse the system for its requirements and possibilities to perform security monitoring and vulnerability management. Specify requirements for security monitoring and vulnerability management in accordance with the respective RCA concepts.
Outputs	Results of monitoring and vuln-management planning documented cybersecurity requirements specification

Table 38 Plan for security monitoring and vulnerability management

7.12.3 Assign responsibilities for organisational and physical requirements

Goals	**Ensure, that organizational and physical requirements are fulfilled in practice by assigning roles and responsibilities**
Phase	5
Inputs	Cybersecurity requirements specification (CRS) Application conditions Physical and organizational countermeasures
Activities	Assign roles and responsibilities for the implementation of the specified physical and organizational countermeasures Document the means to ensure these measures are implemented by those roles.
Outputs	Results of Technical and organizational compensating countermeasures

Table 39 Assign responsibilities for organisational and physical requirements

7.12.4 Establish third party management for security, including supplier security capabilities and support contracts

Goals	**Ensure, that third party security aspects systematically are managed.**
Phase	5
Inputs	Cybersecurity requirements specification (CRS) Application conditions Physical and organizational countermeasures
Activities	Identify and work out necessary contracts with suppliers, to cover third party security management. Identify and work out necessary support contracts with suppliers.
Outputs	Subsystem Cybersecurity Requirements Specification Technical and organizational compensating countermeasures

Table 40 Establish third party management for security, including supplier security capabilities and support contracts

8 Further considerations for CENELEC phase 6-12

This chapter presents further considerations for the phases 6-12 according to EN 50126-1 [11] and prTS 50701 [15]. The phases and tasks descriptions, which are applicable to OCORA are presented in chapter 7.

8.1 Ensuring appropriate degree of personal independence

Goals	**Appropriate degree of personnel independence for tasks that require such independence.**
Phase	6-12
Inputs	-
Activities	Verify that verification tasks are carried out by the defined, responsible role and that role was not involved in the creation of the artefact under scrutiny. The same principles as for the RAMS activities are applied. (c.f. RAM or Safety-Plan).
Outputs	Documentation of verification in phase verification report of respective phase.

Table 41 Ensuring appropriate degree of personal independence phase 6-12

8.2 Maintenance of security related documentation

Phase	Activity
All	Review and update security documentation

Table 42 Maintenance of security related documentation phase 6-12

8.3 System design

Phase	Activity
8	Analyse and identify updates to system design post implementation
9	Verify the applicability of organizational and physical requirements and application conditions Analyse security functionality and requirements coverage
10	Document and finalize cyber security case

Table 43 System design phase 8-10

8.3.1 Analyse and identify updates to system design post implementation

Goals	**Ensure, changes and deviations from the Cybersecurity Requirements Specification of the SuC do not go unnoticed after implementation.**
Phase	8
Inputs	Essential functions (capabilities) of SuC Cybersecurity Requirements Specification (CRS) Breakdown Integration test documentation Automated security test reports

Activities	Review of logical and physical network plans, list of systems and installed applications after implementation Review the system implementation, integration test and automated security test reports to identify deviations from system design and CRS Breakdown. Create a list of security components implemented in the SuC.
Outputs	Updated list of CRS Breakdown including a list of deviations from system realization. List of security components

Table 44 Analyse and identify updates to system design post implementation

8.3.2 Analyse security functionality and requirements coverage

Goals	**Ensure the extent to which cyber security requirements and functionality has been realized by the SuC is understood and documented.**
Phase	9
Inputs	List of security components Integration test documentation Security test reports Updated list of CRS Breakdown including a list of deviations of system realization
Activities	Analyse the documentation as well as the SuC at hand and conclude the extent to which the cyber security requirements have been fulfilled and the necessary cyber security functionality has been realized. Identify remaining open issues.
Outputs	Security Validation report

Table 45 Analyse security functionality and requirements coverage

8.3.3 Verify applicability of organizational and physical requirements and application conditions

Goals	**Verify applicability of organizational and physical requirements and application conditions**
Phase	9
Inputs	List of security components Integration test documentation Security test reports Updated list of CRS Breakdown including a list of deviations of system realization
Activities	Analyse the resulting integrated system and verify the applicability of the defined organizational and physical requirements, are they still applicable and are they being applied? Analyse the resulting integrated system and verify the applicability of the defined application conditions: Are the application conditions still relevant? How are they fulfilled?
Outputs	Security Validation report

Table 46 Verify applicability of organizational and physical requirements and application conditions

8.3.4 Document and finalize Cybersecurity Case

Goals	**Ensure, the rationale and steps for the system under consideration to be secure is documented.**
Phase	10
Inputs	List of security components Integration test documentation Security test reports Verification report Validation report Updated list of CRS Breakdown including a list of deviations of system realization
Activities	After the validation phase the cybersecurity case is made to document the rationale for the system being secure. To this end the structure of the activities defined in the project security management plan are mirrored and for each activity a reasoning for the correct and complete execution is given. (To this end the validation reports shall be helpful.) Besides verification reports and the judgement on these reports, the results of the validation in phase 4 as well as the results of the security validation report in phase 9 are documented in the cyber security case. Finally, remaining open issues, constraints and application conditions are documented.
Outputs	Cybersecurity Case

Table 47 Document and finalize Cybersecurity Case

8.4 Risk Management

Phase	Activity
8	Update risk analysis according to update of system design
11	Update risk management results

Table 48 Risk Management phase 8-11

8.4.1 Update risk analysis according to update of system design

Goals	**New information that may come to light during the design, implementation, manufacture, or procurement stages is taken into account in the risk analysis.**
Phase	8
Inputs	Results and documentation from design, implementation, manufacture, or procurement of the SuC Threat log and risk analysis results
Activities	Review the CRS breakdown and identify differences between specification and implementation. Document these differences.
Outputs	Update of risk management results

Table 49 Update risk analysis according to update of system design

8.4.2 Update risk management results

Goals	**Risk management results are kept up to date throughout the operation phase of the SuC**
Phase	11
Inputs	Previous risk management results
Activities	Verify and if necessary, update the risk management documentation, such that it remains up to date. The frequency of updates depends on the security category of the SuC.
Outputs	Update of risk management results (if necessary, the cybersecurity case)

Table 50 Update risk management results

8.5 Identification, Coordination, and resolution of conflicts

Phase	Activity
6-12	Identify, document, and resolve conflicting measures

Table 51 Identification, Coordination, and resolution of conflicts phase 6-12

8.5.1 Identify, document, and resolve conflicting measures and functional topics

Goals	**Conflicts between RAMS or functional requirements and cyber security requirements are actively managed and documented.**
Phase	6-12
Inputs	Threat risk analysis Threat log Hazard log (safety) and similar results
Activities	Identify and analyse conflicts of security measures with requirements in other areas. Propose different mitigation strategies and resolve conflicts in agreement with the needs of other areas (RAMS, BCM, etc.). Document the results (resolved conflicts)
Outputs	Documentation of resolved conflicts in verification report.

Table 52 Identify, document, and resolve conflicting measures and functional topics phase 6-12

8.6 Process and infrastructure for testing and integration

Phase	Activity
7-11	Execute defined testing measures
12	Disposal of testing-infrastructure taking security criteria into account

Table 53 Process and infrastructure for testing and integration

8.6.1 Update and apply defined procedures

Goals	**Ensure, the testing procedures defined in phase 2 are executed and the results are documented.**
Phase	6-11
Inputs	Test concept and test specifications
Activities	Carry out the tests that were specified (test concept and test specifications). Update the defined procedures if necessary.
Outputs	Test protocols Updated test concept Updated test specifications

Table 54 Update and apply defined procedures

8.6.2 Disposal of testing-infrastructure taking security criteria into account

Goals	**Ensure testing infrastructure is also securely disposed of**
Phase	12
Inputs	Test concept
Activities	Carry out the measures for secure disposal and renewal according to the test concept.
Outputs	Documentation of activities in disposal report

Table 55 Disposal of testing-infrastructure taking security criteria into account

8.7 Verification

Phase	Activity
6-12	The verification step at the end of each phase verifies that all formal requirements of the CENELEC method are satisfied. This means, that all activities have been carried out according to the PSMP and all results have been documented in the way specified by the PSMP. Also for each activity a statement, whether the goal of the activity was reached must be documented by the verifier.

Table 56 Cybersecurity Verification phase 6-12

8.8 Validation

Phase	Activity
9	The phase 9 validation verifies the implementation of the specified cybersecurity requirements as well as organizational and physical countermeasures. It documents remaining, open issues and the exported security related application conditions.

Table 57 Cybersecurity Validation phase 9

8.9 Maintenance, Performance and Operation

Phase	Activity
6,7	Monitor development process and application conditions as they are developed
8	Removal of unnecessary software, hardware, and services Configuration and qualification of security components
10	Review and update business continuity aspects (incl. incidence response and recovery) for the SuC. Define a strategy to maintain SuC in security conditions (identify the most Cyber Critical Assets, define associated strategies for vulnerability watch, testing strategy during operation and maintenance phases, criteria for patching-deployment.
11	Review and test of business continuity aspects (incl. incidence response and recovery) for the SuC Security and vulnerability monitoring Data backup and auditing procedures Maintenance of restrictive access authorizations Application of strategy to maintain SuC in security conditions
12	Disposal of components taking security criteria into account

Table 58 Maintenance, Performance and Operation phase 6-12

8.9.1 Monitor development process and application conditions as they are developed

Goals	**Accompany the development process to prevent surprises (meaning unfortunate ones) in application conditions.**
Phase	6,7
Inputs	Results from the development phases 6 and 7 Cybersecurity requirements specification System design
Activities	As systems and components are developed, also application conditions might be defined by the supplier. These application conditions must be monitored, to ensure the resulting system will not boast application conditions that cannot be fulfilled. To prevent surprises like this, keep an exchange with the supplier and regularly document the state of the status of the known application conditions.
Outputs	Documentation of known application conditions in system design

Table 59 Monitor development process and application conditions as they are developed

8.9.2 Removal of unnecessary software, hardware, and services

Goals	**Ensure proper hardening of the SuC**
Phase	8
Inputs	Documentation of security components
Activities	Analyse the delivered components for unnecessary functionality. Do this independently from the view of the supplier of the system. If eventually unnecessary functionality (software, hardware, and services) is discovered, discuss the reasons why this functionality was implemented with the supplier and if possible, find a way to remove that functionality. Document the implementation of hardening measures and update the SuC's documentation.
Outputs	Updated documentation and hardened components in integration report

Table 60 Removal of unnecessary software, hardware, and services

8.9.3 Configuration and qualification of security components

Goals	**Ensure that security components are configured in the intended way and such that no additional risks are created.**
Phase	8
Inputs	Documentation of security components Cybersecurity requirements specification
Activities	Once security components have been built and delivered, a configuration step might be necessary (e.g., firewall or IDS rules). The security of the components and thus the SuC heavily depends on the correct parametrization of security components. Perform the configuration/parametrization of security components according to the cybersecurity requirements specification (CRS) breakdown. While ensuring, parameters are set within the specified bounds. If there are deviations from the specification necessary, document those deviations as additional risks in the threat log.
Outputs	Parametrized security components in integration report

Table 61 Configuration and qualification of security components

8.9.4 Strategy to maintain SuC in security conditions

Goals	**Ensure that the SuC and the security components are available and up to date.**
Phase	10
Inputs	Cartography of assets Zoning model, threat landscape, risk analysis Testing strategy / categories
Activities	Identify the most Cyber Critical Assets, define associated strategies for vulnerability watch, testing strategy during operation / maintenance phases, criteria for patching or deployment
Outputs	Strategy to maintain SuC in security conditions

Table 62 Strategy to maintain SuC in security conditions

8.9.5 Review and update business continuity aspects (incl. incidence response and recovery) for the SuC

Goals	**Ensure the business continuity aspects remain relevant to the implemented and integrated SuC.**
Phase	10,11
Inputs	System design BCM documentation
Activities	Regularly analyse the BCM documentation for discrepancies with the SuC being operated. If discrepancies are found update the BCM strategy and documentation such that the BCM goals can be fulfilled. This should be done in accordance with the responsible roles for BCM. This activity includes incident response and recovery processes.
Outputs	Updates for BCM documentation and process descriptions.

Table 63 Review and update business continuity aspects for the SuC

8.9.6 Security and vulnerability monitoring

Goals	Ensure adequate security and vulnerability monitoring
Phase	11
Inputs	System design Cybersecurity requirements specification
Activities	Carry out the specified monitoring and vulnerability scanning activities. Regularly verify the procedures and update if necessary.
Outputs	Updated "Cyber Security Case" document from previous phases

Table 64 Security and vulnerability monitoring

8.9.7 Data backup and auditing procedures

Goals	Ensure functioning data backup and disaster recovery processes
Phase	11
Inputs	System design Cybersecurity requirements specification
Activities	Verify and execute the defined backup and auditing procedures for the SuC. Update the procedures if necessary.
Outputs	Updated "Cyber Security Case" document from previous phases

Table 65 Data backup and auditing proceduresMaintenance of restrictive access authorizations

8.9.8 Maintenance of restrictive access authorizations

Goals	Ensure that access authorizations are properly maintained in accordance with the least privilege principle.
Phase	11
Inputs	System design Cybersecurity requirements specification
Activities	Regularly verify compliance with the least privilege principle for granted authorizations. Verify and execute the defined procedures to ensure maintenance of restrictive access authorizations.
Outputs	Updated "Cyber Security Case" document from previous phases

Table 66 Maintenance of restrictive access authorizations

8.9.9 Application of strategy to maintain SuC in security conditions

Goals	Ensure that the strategy to maintain SuC in security conditions engages.
Phase	11
Inputs	Strategy to maintain SuC in security conditions
Activities	Vulnerability watch, testing strategy during operation / maintenance phases, patching-deployment, update residual risks and cybersecurity case.
Outputs	Updated documentation concerned by the application of strategy (technical documentation, residual risks updated of "Cyber Security Case")

Table 67 Application of strategy to maintain SuC in security

8.9.10 Disposal of components taking security criteria into account

Goals	Ensure secure disposal and renewal of the SuC
Phase	12
Inputs	System design Cybersecurity requirements specification
Activities	Dispose of the SuC in accordance with the defined secure disposal procedures.
Outputs	Disposal report

Table 68 Disposal of components taking security criteria into account

END OF DOCUMENT