OCORA

Open CCS On-board Reference Architecture

Security Concept

Document ID: OCORA-TWS06-030

Version: 1.00

Date: 08.06.2022

Management Summary

Industrial systems are affected by an increased threat environment regarding security. Due to an increased threat situation in Europe and the resulting governmental and international requirements, security is becoming more important. The Technical Work Stream 06 (TWS 06) dedicated to Cyber Security addresses this topic in OCORA and will provide detailed requirements for secure CCS systems onboard. The Security Concept paves the way for the future work of TWS 06. It addresses security considerations for the railway domains and defines general security principles. Furthermore, it defines and splits up the systems in the scope of OCORA regarding security. Based on a definition of the threat landscape and attacker types, general security requirements are defined which summarize the results of initial assessments of the work stream. Initial assumptions on the implementation of security service provide an additional insight into the future requirements specifications.

Revision history

Version	Change Description	Initial	Date of change
0.1	Initial draft	MSc	20.09.2021
0.2	Adoptions based on Protection Requirements Analysis, SuC definition, Zoning	MSc; SSt	11.05.2022
0.3	Zoning and Conduit chapter revision	RPo MSc	23.05.2022
0.4	Review comments from GT addressed and figure 5 revision	RPo MSc	24.05.2022
0.5	Final clean-up	RPo MSc	30.05.2022
0.6	Adjusted to new architecture definitions	RPo Msc	01.06.2022
1.0	Official version for Release R2	RPo MSc	08.06.2022

Table of contents

1 Introduction 7

1.1 Purpose of the document 7
1.2 Applicability of the document 7
1.3 Context of the document 7

2 OCORA Security Concept Background 8

2.1 Introduction 8
2.2 Security and safety considerations for Railway Operations 10
2.2.1 Areas of conflict 11
2.2.2 Resolution of conflicts 12
2.2.3 Threat definition 12
2.2.4 System definition 12
2.2.5 Threat analysis 12
2.2.6 Risk analysis 12
2.2.7 Initial Use Case Specification 13
2.2.8 System requirement specification 13
2.2.9 Security Life Cycle Management 13
2.2.10 System architecture, allocation of requirements 13
2.3 Security Principles 13
2.3.1 Secure by Design 13
2.3.2 Defence in Depth 14
2.3.3 Secure by Default 14
2.3.4 Simplicity over Complexity 14
2.3.5 Assume Failure & Compromise 15
2.3.6 Fail Safe and Secure 15
2.3.7 Zero Trust 16
2.3.8 Least Privilege 16
2.3.9 Usability & Management 16
2.3.10 Design for Automation 17
2.3.11 Open Design 17

3 System definition 19

3.1 System under Consideration (SuC) 19
3.2 Threat Landscape 20
3.3 Attacker type definition 20

4 Security Requirements 21

4.1 Protection Requirements Analysis 21
4.2 Architectural Impact Analysis and Requirements 22
4.2.1 Requirements Matrix 22
4.2.2 Understanding the requirements 23
4.2.3 Architectural feedback and improvement 24
4.2.4 Essential components 25
4.3 Zoning and Conduits 27
4.3.1 Process for building zones and conduits 27
4.3.2 High Level zoning concept for the train 27

4.3.3 Detailed Zoning concept for the OCORA scope of the system under consideration 29
4.3.4 Zoning concept of the system under consideration 29

5 Security Services and Supportive Services 30

5.1 Initial Assumption 30
5.2 Security Services 30
5.3 Supportive Services 31
5.3.1 Asset Management 31
5.3.2 Assumption on Maintenance 34

6 Annex 36

Table of figures

Figure 1: Reference EN 50126 and 50701 9
Figure 2: System under Consideration – Physical Transition View 19
Figure 3: System under Consideration - Logical View (based on version of the 31.05.2022) 20
Figure 4: Protection Requirements architectural dependency 23
Figure 5: High level zone concept 28
Figure 6: Zoning and SuC 29
Figure 7: Supportive Services overview 31
Figure 8: Supportive Services SW/Config Update 32
Figure 9: OSS and SSS-TS 34
Figure 10: Assumptions on Maintenance 35
Figure 11: Building Blocks 36

Table of tables

Table 1: Reference Security Documentation 10
Table 2: Areas of conflict (derived from [17]) 12
Table 3: Protection Requirements per Building Block 22
Table 4: Requirements supportive description 24
Table 5 Protection requirements of essential components 26

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

[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-BWS04-010 – Problem Statements

[7] OCORA-TWS01-030 – System Architecture

[8] EULYNX, EUG, RCA, OCORA Security Guideline, Version 2, June 2022

[9] X2Rail-3 – Deliverable D8.2-3c – Protection Profile - OnBoard components, Version 4, 2021-01-28

[10] EN 50126-1:2017-10 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[11] TS 50701:2022 – Railway application - Cybersecurity

[12] IEC 62443-2-1: 2010-11, "Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program", International Electrotechnical Commission (IEC), Edition 1.0, November 2009.

[13] IEC 62443-2-4: 2017-08, "Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers", International Electrotechnical Commission (IEC), Edition 1.1, August 2017.

[14] IEC 62443-3-2: 2020-06, "Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design", International Electrotechnical Commission (IEC), Edition 1.0, June 2020.

[15] IEC 62443-4-1: 2018-01, "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements" International Electrotechnical Commission (IEC), Edition 1.0, January 2018.

[16] OCORA-TWS06-030_Annex_APR – Annex Assessment of the Protection Requirements

[17] Eu.Doc.15 – EULYNX Security Concept

1 Introduction

1.1 Purpose of the document

The purpose of this document is to deliver the content and framework to complete Phase 2 based on TS 50701 and its link to the CENELEC Process V-model. The document shall lay the basis for the next phase, phase 3, the risk and threat analysis. Thus, the main targets are:

1. Definition of generally applicable assumption and definitions
2. Definition of the System under Consideration
3. Protection Requirements Analysis based on the existing system definition and architecture of OCORA
4. Feedback to OCORA to improve system definition and architecture based on the findings in the protection requirements analysis
5. High level requirements definition to the building blocks defined in the architecture

This document is addressed to experts in the CCS domain dedicated to architecture, network, safety functions and security functions and to any other person, interested in the OCORA concepts for on-board CCS. The reader 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 on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

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

1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of an OCORA release, together with the documents listed in the release notes [1]. 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 OCORA Security Concept Background

2.1 Introduction

In reference to the relevant standards EN 50126 [10], TS 50701 [11], IEC 62443 [12] as well as the EULYNX/RCA/OCORA guideline for cyber security [8]. The following introduction to the overall security process and its references will be provided. This will ensure future proof of the overall security concept for the evolving connectivity between infrastructure and rail vehicles.

The EN 50126 understands “security” as resilience of the railway system to vandalism, malevolence, and intentionally harmful human behaviours. 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 [10], to apply the security engineering processes proven in other industries, e.g., IEC 62443 [12].

The standard TS 50701 [11], documents the interaction of safety and security. As a result, the detailed steps of a security engineering process are following the V-model. The security engineering process will 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., in the cyber security case and are gaining granularity during the later EN 50126 [10] phases (see Figure 1).

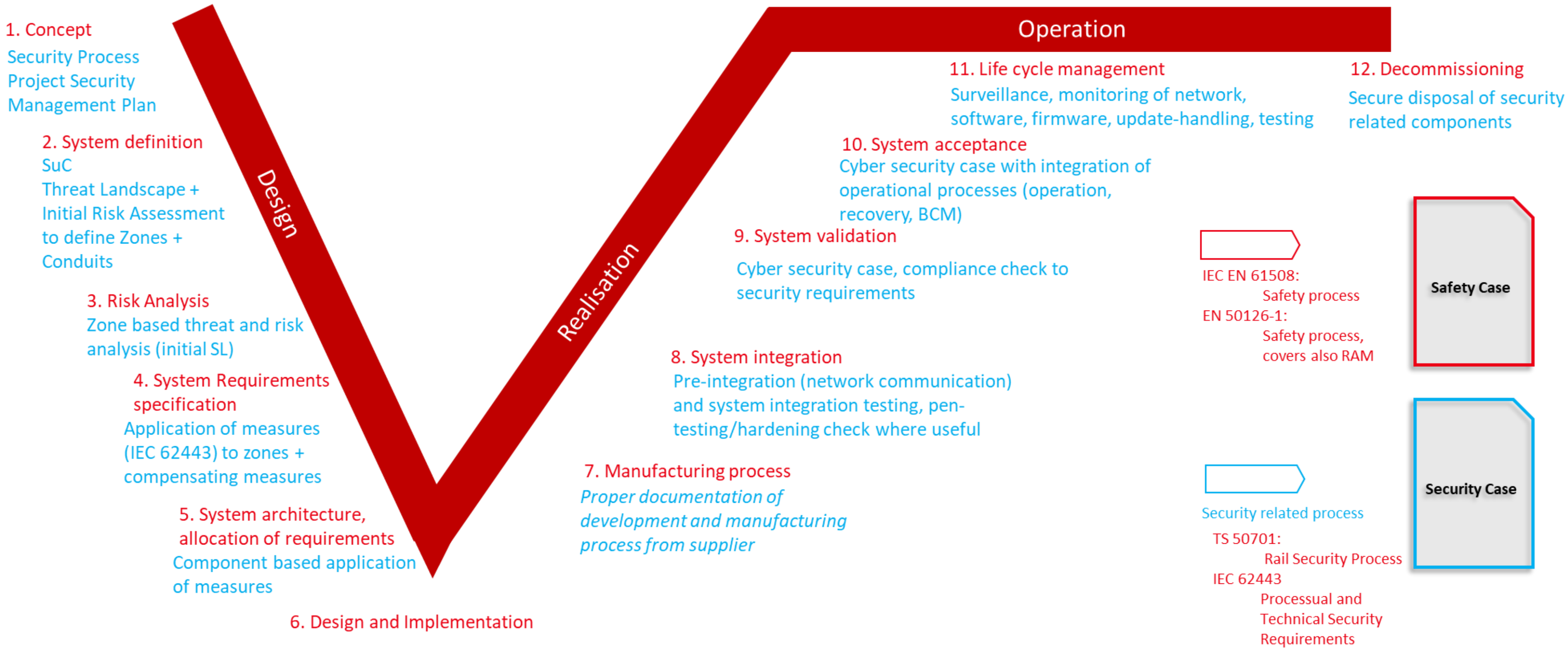

Figure 1: Reference EN 50126 and 50701

The security engineering process will cover the System under Consideration (SuC), its interfaces, and relations to surrounding systems. These systems may be in similar technology or maturity level as the SuC. It is also possible that interfaces to already established, maybe outdate, and so-called legacy systems need to be considered.

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

Security solutions shall not be subject to safety assessment in contrast to railway solutions, which are developed according to EN 50126 [10]. Therefore, the process of security engineering can be passed through separately. However, synchronization is necessary to ensure the coordinated transfer of input and output. Each phase of an EN 50126 [10] project has an equivalent in the V-model.

All security documents are classified to the V-model and one or more corresponding applications (EULYNX, RCA, OCORA).

Document Identifier	**Title**	**Status**	**CENELEC**	**EULYNX**	**RCA**	**OCORA**
OCORA-TWS06-010	Project Security Management Plan	R2 released	1			x
-	Security Guideline	R2 released	2-5	x	x	x
OCORA-TWS06-030	OCORA Security Concept	R2 released	2	x		
OCORA-TWS06-040	OCORA Security: Threats and Risks Analysis	Future release	3	x		
OCORA-TWS06-050	OCORA Security Specification	Future release	4,5	x	x	
Eu.Doc.115	Security parameter specification	BL 4 released	4,5	x	x	x
Eu.Doc.117	SSI Standard Security Interface	BL 4 released	4,5	x	x	x

Table 1: Reference Security Documentation

2.2 Security and safety considerations for Railway Operations

The OCORA security documents are based on following assumptions on areas of conflict in safety and security which result in the overall concept as “resolution of conflicts.”

2.2.1 Areas of conflict

	Safety	Security
Trust vs. Zero trust	Unconditional trust within the whole system. The system was designed and tested/certified by a competent body. All aspects considered correctly. If the operator follows the requirements (technical, processual, controls), nothing bad can happen. Everyone is acting as requested!	Miss-trust / Zero trust No trust until a defined level of trust is established. There are people intentionally not following the requirements (e.g., to ease their work or to attack).
Fail Safe & Secure	The system never should harm itself or the environment. In case of doubt or failure it enters automatically into a "safe state." It is based on Safety Integrity Levels provided by established standards.	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. Primary goal is ensuring system's integrity.
Monitoring & Logging	Detecting errors/failures is time critical as safety might be affected. There are only technical failures and considered wrongdoings. All safety-relevant failures are detected, a timely reaction is performed, or initiated, by the system itself or by the superior system.	Systems are monitored to detect failures with respect to operational levels/availability. The log data might indicate an attack or other security problems.
Defence in Depth	There are no attackers. The whole system is in a controlled environment. Intentional wrongdoings are excluded.	There are attackers, from outside and inside. Every (sub-) system must establish the security controls on several layers to protect against outside and inside attacks (including lateral attacks).
Simplicity over Complexity	Safety relevant systems are designed only for that very task, only contain the minimum required to implement the defined safety functionality.	Security systems must be tailored to the task as these systems/libraries include many options. The systems are highly complex and as a result faulty. The tailoring is done usually during system integration and not during the design phase. This tailoring changes over time due to changing threat landscape.
Assume failure and compromise	Failure states are detected in a timely manner. Compromising a system is impossible due to requirements and controls.	It is very likely that an attack is not detected in a timely manner. Compromising a system is possible all the time. Both could potentially be detected years later.
Open Design	Highly integrated, proprietary/closed designed systems. 100% control of the system and its design reduces the risk in the approval process. The supplier guaranties the safety functionality and spare parts for decades.	Open standards and designs are preferred. Close or proprietary protocols and interfaces are per se considered insecure, as no independent testing can take place.

	Safety	Security
Maintainability / Availability / Updates	There is no need for updates if everything was considered correctly, and the test procedures were not faulty. The system is operated in a deterministic environment, hence there are no unconsidered coincidences. Every change requires a new certification/homologation.	As attack vectors change over time, updates are required. Newly detected security vulnerabilities must be mitigated. Both requires to updating system and protective concepts. This is the only way to ensure system/information integrity.

Table 2: Areas of conflict (derived from [17])

"Fail secure" or "fail safe" affects availability negatively. For a safety system, system integrity is key and is the basis for all assessments and certifications. A "fail open" action can therefore never be accepted for safety or safety-related systems or functionality. Depending on architecture and technical implementation, a "fail open" is only acceptable, if system integrity for safety is not affected and ensured by design of the system.

2.2.2 Resolution of conflicts

As the areas of conflict cannot be eliminated in general, the analysis of all RAMSS aspects must be done together. The method of “separation of concerns” can be followed if interactions/conflicts are identified and solved. Defining them as out-of-scope is not an option.

Security must start with the information used end-to-end, e.g., this is the top-level control loop if a System-Theoretic Process Analysis (STPA) method is applied and following the information flow defined by the processes. These processes involve business delivery processes and operational technology control loops.

As security affects safety and RAM aspects, a security protection profile must include all RAMS aspects, hence there is only one protection profile.

2.2.3 Threat definition

In OCORA, coordinated with EULYNX, EuG and RCA, the term “threat” is used to denote a negative impact to the assure ability of the OCORA solution. This is not to be confused with the use of “threat” in the security domain. Therefore, in this document we refer to both Assurance Threats and Security Threats.
If not otherwise stated, the term “threat” in this document refers to a Security Threat.

2.2.4 System definition

The SuC provides the architecture overview including sub-systems, interfaces, and the system boundaries. It also describes the responsibilities within the system boundaries. The architecture defines the communication network, security zones and conduits. It also includes the generic system functions and takes the security aspects, as well as the safety aspects into account to fulfil the regulatory requirements and limit initial risks.

Basis for the system definition is a structural analysis of the system to identify all components that are included in the communication regarding the train functions. Furthermore, all access points to the system (physical or logical) need to be identified. The system definition is part of the security concept.

2.2.5 Threat analysis

The threat analysis provides an overview on the possible threats for the System under consideration.

2.2.6 Risk analysis

The separate risk analysis document performs the zone and conduit-based risk assessment including a detailed threat analysis, hazard log, and mitigation controls.

The identification of the current risks, threats, hazards, and vulnerabilities will lead to an initial security level documentation. Within the risk evaluation also mitigation measures will be considered.

2.2.7 Initial Use Case Specification

The use cases specification includes predictable use cases that need to be performed to allow the security incident detection through the connected Security Information and Event Management (SIEM). This is needed to derive the requirements for each component and to ensure that the relevant information is available. The use case specification will not include exact definition of the use case implementation or correlation process. This is performed by the SIEM security specialists later with the onboarding process.

2.2.8 System requirement specification

In this chapter we will perform a SuC-specific refinement of system requirements. Including definition of organizational and physical requirements and security-related application conditions. Here we describe how the requirements should be implemented/applied, to be compliant with the security and safety standards.

2.2.9 Security Life Cycle Management

The Life Cycle Management delivers the relevant processes to ensure the system security over the lifetime through patch and test process definition. The relevant capabilities are foreseen in the requirement specification already.

2.2.10 System architecture, allocation of requirements

Allocates the security requirements to the (sub-)systems, components, and interfaces.

2.3 Security Principles

The security principles used in this concept are listed in the following chapters and are based on IEC 62443-4-1[15].

2.3.1 Secure by Design

Make security part of requirements and lifecycle definition, and not an afterthought

Rationale
Protect a 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 behaviour) they must be a holistic approach

Implications

- Understand the resulting security requirements in the engineering, design, implementation, and disposal of the system
- Make use of strong keys (as strong as operational useable - this is a moving scale in time and available computing power)
- Security should treat the root cause of a problem, not its symptom. Security incidents should be avoided by design.

2.3.2 Defence in Depth

Avoid reliance on a single type of security control

Rationale
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 effort for an attacker to compromise a system or application

Implications

- Create a security architecture that documents the different layers of protection
- Balance defence in depth against simplicity and business needs
- Each deeper 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

2.3.3 Secure by Default

Use secure default options to limit inherent security vulnerabilities

Rationale
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 to work and should just work reliably were implemented
- 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 integrity protection and encryption by default for both data at rest and in transit. Encryption can be omitted if confidentiality protection is not required.

2.3.4 Simplicity over Complexity

Complexity is the worst enemy of security

Rationale
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, the more likely it may possess exploitable flaws

Implication

- Simplicity should be a key objective in design of systems and security
- DRY - do not repeat yourself
- Reduce the variety and types of hardware and software types and versions
- Designing systems that use the least hardware and software resources possible
- Favour 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 once we find them
- Loosely coupled, low complexity. Create process chains (security zones) with as much independence from other security zones as possible.

Notes

- Do not over-simplify
- Balance reduced complexity against diversity required to achieve resiliency and reduced single-point-of-failures

2.3.5 Assume Failure & Compromise

Complex distributed systems lead to unpredictability and cascading failures

Rationale
We build and operate highly coupled and interactively complex systems. 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 difficult to predict. Prediction, complete testing, and modelling of all states is not possible in such systems, we therefore 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 can be compromised during the life cycle of the components and systems
- Embrace principles of resilient 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
- Security shall actively manage over the IACS and product life cycle

2.3.6 Fail Safe and Secure

Failures should lead to a safe and secure state. Risk does not hurt - the impact does

Rationale
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 isAuthorized(), isAuthenticated(), and validate() should all return false if there is an exception during processing

- Assume system failure & compromise in design decisions

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.

2.3.7 Zero Trust

Assume everything to be insecure until a level of trust is established

Rationale
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, 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 its systems 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

2.3.8 Least Privilege

Only grant the minimal set of permissions that are necessary for a required/given operation/action - and no more

Rational
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 time out

2.3.9 Usability & Management

Balance of security and usability - make secure behaviours easy instead of complex

Rationale
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 interface must be easy to use, so that users routinely and automatically apply the mechanisms correctly. 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

2.3.10 Design for Automation

Design for Automation to control complexity

Rationale
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

2.3.11 Open Design

The security of a mechanism should not depend on the secrecy of the details of its design or implementation

Rationale
Assume outsiders and attackers will have access to source code (also for closed source software), system 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 enemy knows the system

3 System definition

The system definition covers the definition of the system under consideration and an initial threat analysis to allow building zones and conduits.

Currently no OCORA System Definition is available. The CENELEC phase 1 document and the OCORA System Architecture are the only sources for defining the system.

Therefore, the system definition, which defines the base for the security considerations is built by the two following documents and assumptions made during the activities:

[1] OCORA-TWS01-030 – System Architecture

[2] OCORA-TWS10-010 – CENELEC Phase 1 – Concept

The assumptions made during the considerations and assessments need to be revisited after the OCORA System Definitions becomes available. All the assumptions need to be well documented and evaluated if they are still valid in a later phase of OCORA. Eventually the status of an assumption varies, so a tailored process needs to be defined to manage this issue.

3.1 System under Consideration (SuC)

The definition of the OCORA system is a task performed by TWS01 System Architecture [7] ((based on the version of the 31.05.2022)

from an architectural point of view.

The following figures presents the SuC used in TWS06 Security.

Figure 2 show the physical components and networks which are used during the transition to future OCORA systems.

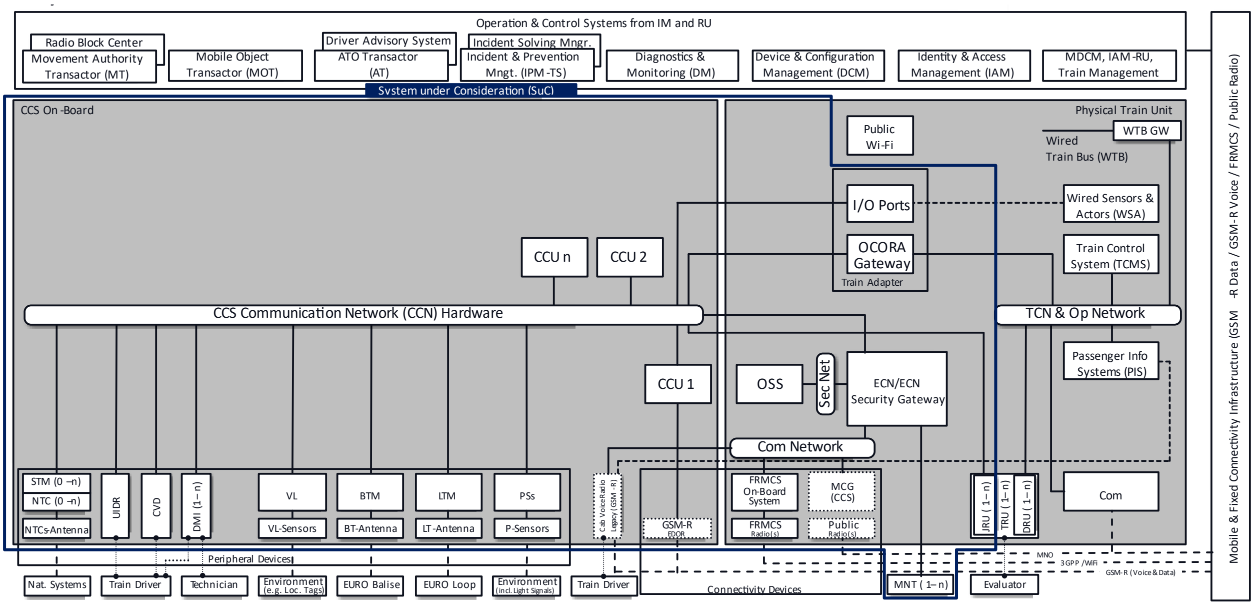

Figure 2: System under Consideration – Physical Transition View

The logical connections of all systems according to the system view is shown in Figure 3.

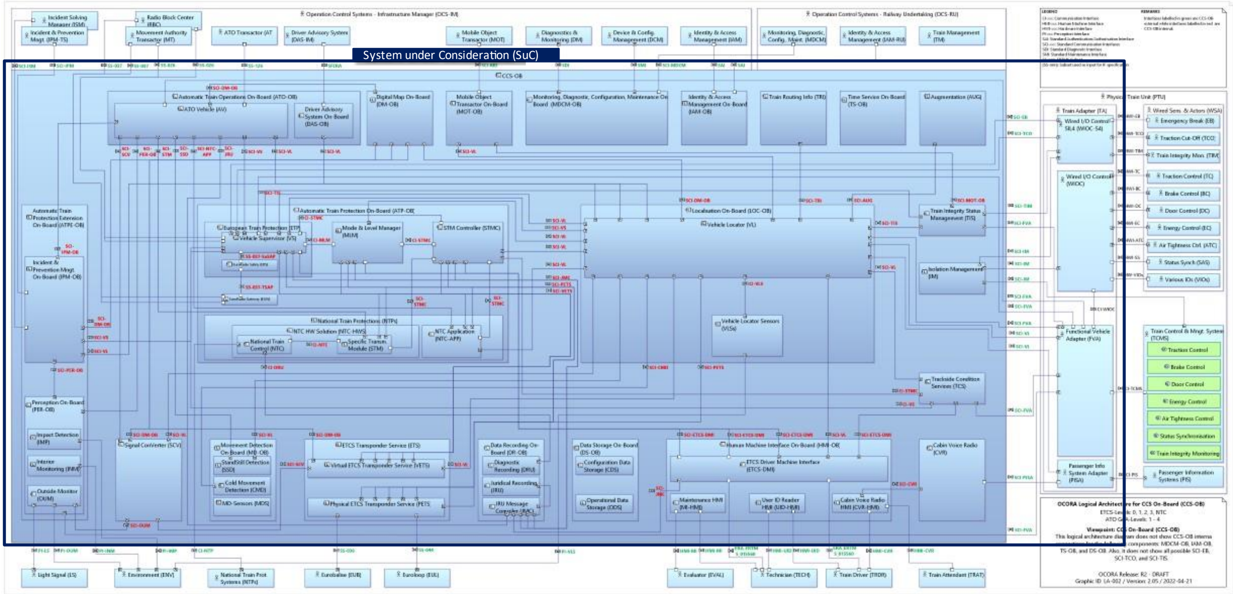

Figure 3: System under Consideration - Logical View (based on version of the 31.05.2022)

The basis of the SuC definition is the OCORA logical architecture and the physical transition view from the OCORA System Architecture [7]. Please note that the architecture view used in this concept provided by TWS01 to TWS06 has not been published and was altered for R2.

From security perspective it is essential to take the whole train into consideration to create comprehensive security measures to protect the operational relevant systems against attacks. Therefore, the system under consideration is covering not only CCS On-Board (CCS-OB) but also the Train Adapter, ECN/ECN-Security Gateway and dedicated communication and security components.

Also, all possible train compositions and vehicle types must be considered during the security related considerations respectively analyses and measure management, because of the different implementations.

The TCMS components, WSA (wired sensors and actors) and PIS components are outside the SuC and are not considered by TWS 06.

The interfaces to the WSA are highly proprietary, therefore TA and WIOC needs to be developed for each train fleet by the specific vendor.

Only the interfaces specified by OCORA are considered.

3.2 Threat Landscape

The threat landscape is relevant for the risk and threat analysis (phase 3) and thus part of the Secuity Guidelines [8].

3.3 Attacker type definition

The attacker types will be defined, and the exclusion of attackers will be assessed for R3.

4 Security Requirements

4.1 Protection Requirements Analysis

The basis for building zones and conduits is an initial definition of level of needed security based on possible threats and security goals (protection needs). Therefore, the logical architecture is analysed with a protection requirements analysis (APR).

The APR uses the following criteria to analyse the protection requirement per interface. These criteria cover all protection targets relevant for the OCORA domain:

1. Confidentiality
2. Integrity
3. Availability
4. Non-Repudiation
5. Authenticity (only Human-Machine interface)

The criteria are classified based on the following levels:

- Low
- Middle
- High
- Very High

Per interface only one level is defined. The definitions of these levels are available to the OCORA members. The maximum level of the evaluation of the five criteria is documented. The made assumption are explained in the APR document [16].

To ensure consistency in the analysis of the protection requirements and the use of levels a risk matrix is used that allows to comprehensively analyse possible impacts.

The protection requirements per building block [7] are displayed in the following Table 3. Please note that the building block definition used in this concept provided by TWS01 to TWS06 has not been published. The building block definition used for this assessment is shown in Figure 11.

Building Block	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
AUG	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
AV	Not relevant	Middle	Low	Low	Not relevant
CMD	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
CVR	Not relevant	Very High	Low	Middle	Not relevant
DAS-OB	Not relevant	Low	Low	Low	Not relevant
DM-OB	Not relevant	Very High	High	Middle	Not relevant
EGW	Not relevant	Very High	Low	Middle	Not relevant
ETCS Core	Not relevant	Very High	High	Middle	Not relevant
External	Very High	Very High	Low	Middle	Very High
HMI-OB	Not relevant	Very High	Middle	Middle	Very High
IAM-OB	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IPM-OB	Not relevant	Very High	Low	Middle	Low
LOC-OB	Not relevant	Very High	High	Middle	Not relevant
MDCM-OB	Very High	Very High	Low	Middle	Very High
MOT-OB	Not relevant	Very High	Low	Middle	Not relevant
n/a	Not relevant	High	Low	Middle	Not relevant
NTPs	Not relevant	Very High	High	Middle	Not relevant
PER-OB	Not relevant	Very High	Low	Middle	Not relevant
PTU-External	Not relevant	Very High	Middle	Middle	Not relevant
SCV	Not relevant	Very High	Low	Middle	Not relevant
TIS	Not relevant	Very High	High	Middle	Not relevant
TRI	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
VETS	Not relevant	Very High	Low	Middle	Not relevant

Table 3: Protection Requirements per Building Block

The detailed requirements per logical component and interface are displayed in the protection requirements analysis [16].

4.2 Architectural Impact Analysis and Requirements

4.2.1 Requirements Matrix

The development of a system architecture is an iterative process. Further, OCORA foresees different integration phases to allow improving existing vehicles, those that are going to be delivered in near future based on older requirement set-ups and future systems that meet the OCORA target set-up.

To support the iteration and migration process, the impact of different solutions to the security analysis and protection needs shall be flexible adoptable without analysing each possible variant. That is why a requirements definition was made that allows to understand the impact of architectural decision to the security requirements.

The matrix (Figure 4) represents the principle of the full requirements set-up in [16]. Figure 4 is a shortened excerpt of the full matrix. It shall be used the following way:

Preconditions:

- There is a given architecture. In this case, it is the OCORA logical architecture with the building blocks
- A protection requirements analysis was performed before, following the principle of chapter 4.1.

How to interpret the result and what to expect:

The matrix shows how the requirements change if an interface with a certain protection requirement moves from internal interface (connecting components inside one component via an physical protected network) to an external (connecting components via open/unprotected networks) interface and further distinguishes between the type of external connection.

The matrix does not represent a full set of security requirements per component or system, but only concentrates on the main differences.

The matrix comprehensively shows a system architecture together with his security and safety experts what consequences architectural decisions have.

This matrix shall support a carefully chosen architecture that allows to meet the following requirements:

- Efficient (financial)
- Efficient operation
- Manageable over the life cycle
- Minimise OT-security risks

How to read the matrix:

1. The analysis on an existing architecture was done interface per interface or component per component
2. First the interface is classified to the greyish categories, e.g., external, wired connection
3. Second the relevant protection requirement is chosen, e.g., Confidentiality
4. Third the protection level is identified from the APR, e.g., medium
5. Fourth the meeting point of the column of the protection level (e.g., medium) and the connection category (e.g., external wired) displays the requirement differentiation criteria (e.g., AES 256 encryption and endpoint authentication)

		APR highes requirement from **Confidentiality**	
		low	medium
component	**data (information) at rest and software**	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening
	SW 2 SW comm. (pure internal)	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening
Connection type	**internal network**	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication
	wired (external)	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication
	radio (external)	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication

Figure 4: Protection Requirements architectural dependency

In [16] the full matrix is available covering all protection requirements and level of protection from the APR in chapter 4.1.

4.2.2 Understanding the requirements

The requirements from chapter 4.2.1 are, as described, only those requirements that differentiate between different architectural decisions. The full set of requirements will be derived from the threat and risk analysis in phase 3. The full set of requirements to the building blocks, based on the APR and phase 2 is presented in this document.

Following context is given to every of these differential requirements, to allow to use it properly for architectural design or component/system development.

The requirements are grouped. So e.g., “encryption end to end with endpoint authentication” is only explained once, the difference of AES 128, AES 256 is assumed to be comprehensive to the reader. Table 4 gives more context for some of the requirements to understand the impact of the distinction.

Requirement	Additional comment
Encryption end to end with endpoint authentication	Here AES encryption methods (symmetric) are defined. It is assumed that the key exchange process is asymmetric.
The developer must consider security with respect of implementing SL-T and expected attacker category.	This implies that the organization of the developer knows the relevant processes and works in well-defined processes according to IEC 62443-4-1 [15], IEC 62443-2-4 [13] and IEC 62443-2-1 [12] (depending on the organization)
Monitoring/detection of malware (SIEM) with central logging	It is assumed that security monitoring and intrusion detection is implemented onboard. Further it is assumed that events are event driven sent to the land side in a back-end SOC to be treated within an incident response process. In addition, security logging information shall be available constantly on the SOC (back-end) side to allow a continuous overview of the threat landscape.
Protect component availability low	The definition of low, middle, high, very high is to be defined by the operator. An assumption was made in the protection requirements analysis.
Two radio networks with own core or high availability one-network-design; with automated detection of availability load handling and "switching" between networks; or combination radio and wired networks	Very high availability requirements via a radio connection are assumed nearly impossible as radio connection can be easily and remotely interrupted, e.g., through jamming.
Multi-network, multi-source, multi-operator (not service provider, operator!) with automated detection of availability load handling and "switching" between networks + cabled network or "wire breakage proof" required (process resilience to connection interruption)	
Username, no or weak password; roles for authorization	Authenticity in the protection requirements is only analysed for human-machine interface. This is because authenticity in machine-2-machine communication is state of the art and independently from the network design required by IEC 62443.

Table 4: Requirements supportive description

4.2.3 Architectural feedback and improvement

Based on the System Requirements of the IEC 62443 the R2 architecture of OCORA is assessed. The SRs will be selected and assigned as mitigating measures in the risk assessments for R3. To prepare this process and to identify possible conflicts of system requirements and the current OCORA architecture as early as possible, a conflict check has been performed. This conflict check takes all SRs relevant for SL 3 into account. The result can be used in two different ways:

- Input to the architecture of R2

  Some conflicts with the SRs have already been resolved by the architecture workstream. Thus, some aspects of the OCORA security are aligned as early as possible.

- Mitigating measures for the risk assessment of R3

  The upcoming risk assessment of R3 will take SRs into account and use them as mitigating measures.

During the assessments, the identified applicability can directly be used, which helps to improve the risk values and evaluation of mitigating measures.

This IEC 62443-3-3 check is not published, but some changes have been included in architecture of R2 already due to collaboration of TWS06 Security and TWS01 Architecture. These changes include amongst others:

- Cabin Voice Radio

  The Cabin Voice Radio component is connected through the Security Gateway and has no direct connection to the CCN anymore.

- MT (Maintenance Terminal)

  The Maintenance Terminal will not have direct access to the CCN and is connected through the Security Gateway.

Furthermore inter alia following open topics have been identified and will be addressed in future releases:

- Identity and Access Management
- Account and Authorization Management
- Network Segregation
- DMI and User Authentication
- Software and Configuration Updates
- Isolation and Degraded Mode

4.2.4 Essential components

In accordance with TS 50701 essential functions shall be determined to allow focus on the systems and components with the highest protection needs for integrity, as they support most the safe process of the rail system. As OCORA has defined an architecture with logical components, this method is applied to these logical components

The following table shows the essential components of the logical architecture in OCORA.

Component	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
CVR	Not relevant	Very High	Low	Middle	Not relevant
CVR-HMI	Not relevant	Very High	Low	Middle	Not relevant
DCM	Very High	Very High	Low	Middle	Very High
DM	Very High	Very High	Low	Middle	Very High
DM-OB	Not relevant	Very High	High	Middle	Not relevant
EGW	Not relevant	Very High	Low	Middle	Not relevant
ERS	Not relevant	Very High	Low	Middle	Not relevant
ETCS-DMI	Not relevant	Very High	Middle	Middle	Not relevant
FVA	Not relevant	Very High	Middle	Middle	Not relevant
IPM-OB	Not relevant	Very High	Low	Middle	Low
MDCM	Very High	Very High	Low	Middle	Very High
MDCM-OB	Very High	Very High	Low	Middle	Very High
MI-HMI	Not relevant	Very High	Low	Middle	Very High
MLM	Not relevant	Very High	High	Middle	Not relevant
MOT	Not relevant	Very High	Low	Middle	Not relevant
MOT-OB	Not relevant	Very High	Low	Middle	Not relevant
MT	Not relevant	Very High	Low	Middle	Not relevant
NTC	Not relevant	Very High	Low	Middle	Not relevant
NTC-APP	Not relevant	Very High	High	Middle	Not relevant
PER-OB	Not relevant	Very High	Low	Middle	Not relevant
PETS	Not relevant	Very High	Low	Middle	Not relevant
PISA	Not relevant	Very High	Low	Middle	Not relevant
RBC	Not relevant	Very High	Low	Middle	Not relevant
SCV	Not relevant	Very High	Low	Middle	Not relevant
SSD	Not relevant	High	Low	Middle	Not relevant
STM	Not relevant	Very High	Low	Middle	Not relevant
STMC	Not relevant	Very High	High	Middle	Not relevant
TECH	Not relevant	Very High	Low	Middle	Very High
TIS	Not relevant	Very High	High	Middle	Not relevant
VETS	Not relevant	Very High	Low	Middle	Not relevant
VL	Not relevant	Very High	High	Middle	Not relevant
VLSs	Not relevant	Very High	Low	Middle	Not relevant
VS	Not relevant	Very High	High	Middle	Not relevant
WIOC	Not relevant	High	Low	Middle	Not relevant
WIOC-S4	Not relevant	Very High	Low	Middle	Not relevant

Table 5 Protection requirements of essential components

4.3 Zoning and Conduits

4.3.1 Process for building zones and conduits

The Protection Requirements analysis has analysed the kind of protection need per interface and/or component.

Based on the protection requirements components are grouped into zones and conduits. The zoning process is briefly described with examples in IEC 62443-3-2 [14].

Zones in the context of IEC 62443, TS 50701, the Security Guideline [8] and thus this Security Concept always mean Security zones. This is different from network zones and not equal or similar.

The following rules are defined and applied:

Zones are:

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

Conduits connect:

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

The zoning is documented in the protection requirements table based on the protection requirements and graphically displayed in the architecture.

The results of the zoning and protection requirements show:

- the distribution of crucial functions in the architecture
- criticality of the protected functions

This allows a discussion in the sense of safety and security and the necessary approvals, safety, and security levels. The feedback should be used to improve the architecture to reduce the critical interfaces and components to a minimum.

Based on the zoning, in phase 3 (Threat and risk analysis) the SL-T shall be defined per zone.

The detailed protection requirements analysis concentrated on the CCS system only. Nevertheless, a full overview of the train is relevant to set the CCS system and its zoning concept into relation of the full train. Therefore, based on Shift2Rail X2Rail-3 High-level on-board security architecture [9] and the protection requirements analysis the zoning concept is split in a high-level zoning in chapter 4.3.2. and a detailed zoning concept (sub zones) in chapter 4.3.4.

4.3.2 High Level zoning concept for the train

Based on the different protection needs and fundamentals like commonly used vehicle architectures and zoning examples provided by the standards, the train system is split into four main zones for the security analysis.

- Train Signalling and ATP zone
- Train Control and Command Zone
- Train Auxiliary Zone
- Train Public Services Zone

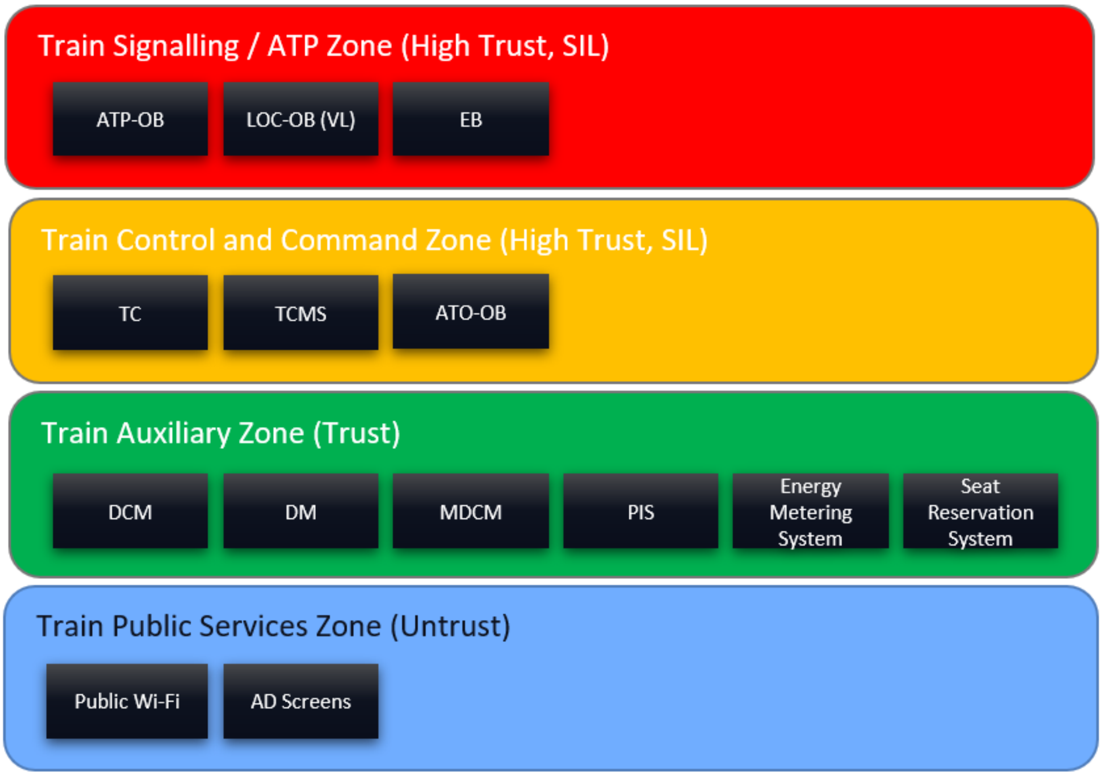

Figure 5: High level zone concept

The mapped functions per zone represent the most applicable to the specific zone and are examples, as the system definition in OCORA for the full train is not defined as complete, yet.

In the next step the high-level zone concept is distributed to the train system. As OCORA does not define one future solution for the train, the following description represent the principles that shall be used for zoning of train systems.

1. Zones containing the same type of systems and accordingly same protection requirements can be present in multiple locations in the train.
2. Zones with same protection requirements in different locations of the train can be merged to one zone, if:

   the communication path between the two locations can't be accessed by an abuser due to the type of cable routing or physical protection
3. Zones with same protection requirements in different locations of the train cannot be merged to one zone and thus are connected through conduits, if:
   a. The communication path between the two locations can be accessed by an abuser, for example through network devices (switch, router, access point), accessible cable connection or wireless connection
   b. The communication path is not permanent but can be unplugged, for example between two train sections

In the example it is assumed that:

1. All components/systems with same protection requirements at one location can be grouped into one zone, as they can be protected physically and logically accordingly.
2. All zones with same protection requirements with different locations in the train cannot be grouped into one zone as the connection is based on Ethernet with support of network devices that are easily accessible (low physical protection) throughout the train.

4.3.3 Detailed Zoning concept for the OCORA scope of the system under consideration

The zoning of the OCORA System under Consideration is mainly derived from a functional point of view considering criticality of assets and logical location as recommended in [14]. The zoning corresponds also to the X2Rail-3 High-level on-board security architecture [9] and the TS 50701 Railway physical architecture model. The OCORA zoning concept is shown in Figure 6.

4.3.4 Zoning concept of the system under consideration

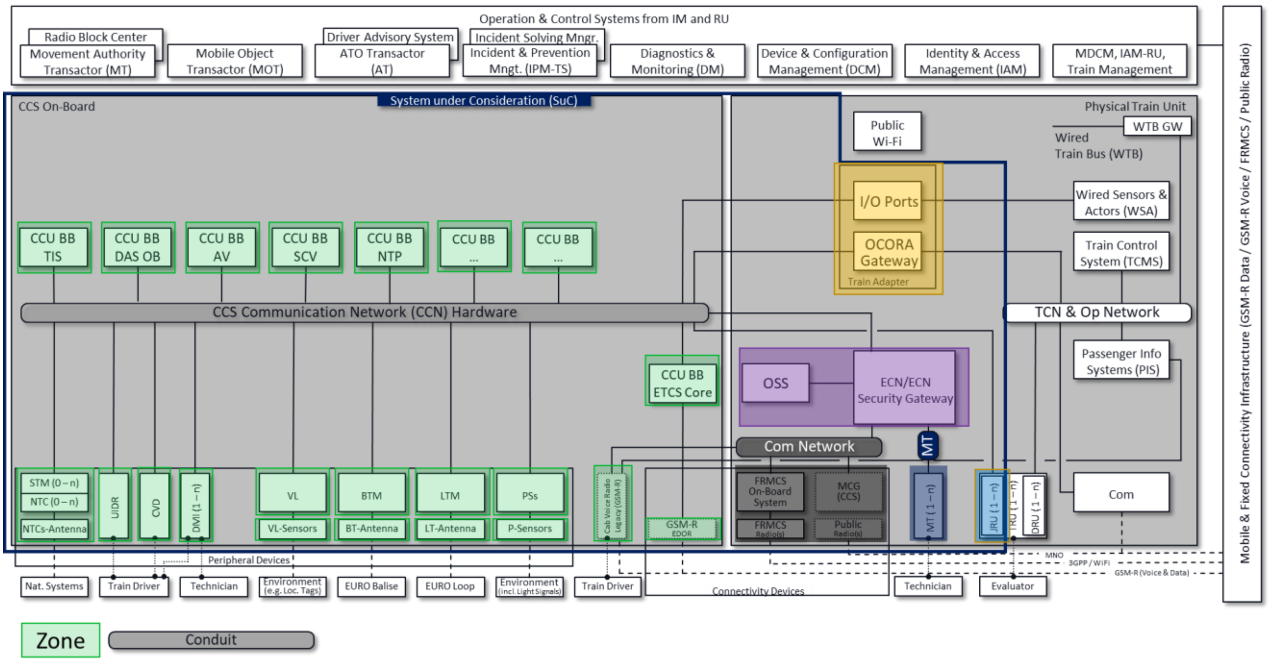

Figure 6: Zoning and SuC

The status of the OCORA project (phase 2) shows, that the logical connections/components, and the system architecture are not finally designed. Furthermore, the functional scope is not completely defined yet. The logical and physical components are later combined in building blocks (BB). These building blocks will probably be mapped to implemented components.

Due to these aspects, it is not possible to define a final zoning. Only the preliminary system under consideration can be defined. Additionally basic assumptions on a zoning concept based on a stable architecture for a future release can be defined.

The current SuC is based on the transition view and other versions of the OCORA architecture are currently not considered. The SuC is shown in Figure 6 and includes all the CCS and supporting components. The TCMS and external systems are excluded.

The zoning is shown above is based on the following assumption:

- Each BB is represented by one CCU
- Each CCU is part of one zone
- Sensors/Antennas and CCUs are separated in different zones
- Security Gateway is in the same zone as the connected OSS

  (The functionality of the Security Gateway could be split up in multiple security components in a future architecture. Furthermore, more than one Security Gateway could be implemented.)
- The Train Adapter and the included Gateway is an own zone

CCUs are added to separate zones, as they can be physically located in different parts of the train. If CCUs are combined to one component it can also be combined to one zone. The highest protection requirements of all combined zones are used for combined zones.

Currently the following zones are defined:

- Train Adapter (orange)
- JRU (light blue)
- MT (dark blue)
- OSS and SecGw (purple)
- Com (black)
- Unspecified BB/CCU/sensor zone – one zone per CCU/BB/sensor (green)

The Train Adapter is a separate zone, as it does not directly transfer, but convert data.

The following conduits exist:

- CCN (grey)
- Com Net (black)
- MT Net (dark blue)

The CCN-conduit can be split up in separated and individual conduits depending on the implemented architecture.

Additional conduits (e.g., Sensors/Antennas to CCUs) can be defined, but are not assessed yet due to the instable architecture.

The Security Gateway represents the perimeter protection of the zones and is connected on the OSS in one zone, as both fulfil security functionalities together.

5 Security Services and Supportive Services

5.1 Initial Assumption

It is assumed that, based on the threat and risk analysis (phase 3), the security services and supportive services will be required. Thus, they are presented as input in the Security Concept already to be considered in the further architectural development.

5.2 Security Services

The security services are standardized between EULYNX, EUG and OCORA and further coordinated with Shift2Rail X2Rail3.

Security services serve as central services over the life cycle. Standardization supports easy implementation and interoperability.

The specification of the security services is available in EU.Doc.117 (Security Services Interface) and EU.Doc.121 (Security Services Platform).

The services are:

- Time
- Back-up

- SIEM
- Security Logging
- PKI (Public Key Infrastructure)
- IAM (Identity and Access Management)

Further description and details are not given to ensure single source usage.

5.3 Supportive Services

Supportive services enable security services, safety services and maintenance over the life cycle.
The following supportive services shall be in place:

- Asset Inventory
- Software and Configuration Repository
- Diagnostic Logging

Their general interaction and connection are displayed in Figure 7. The supportive services are each described in more detail in the following chapters.

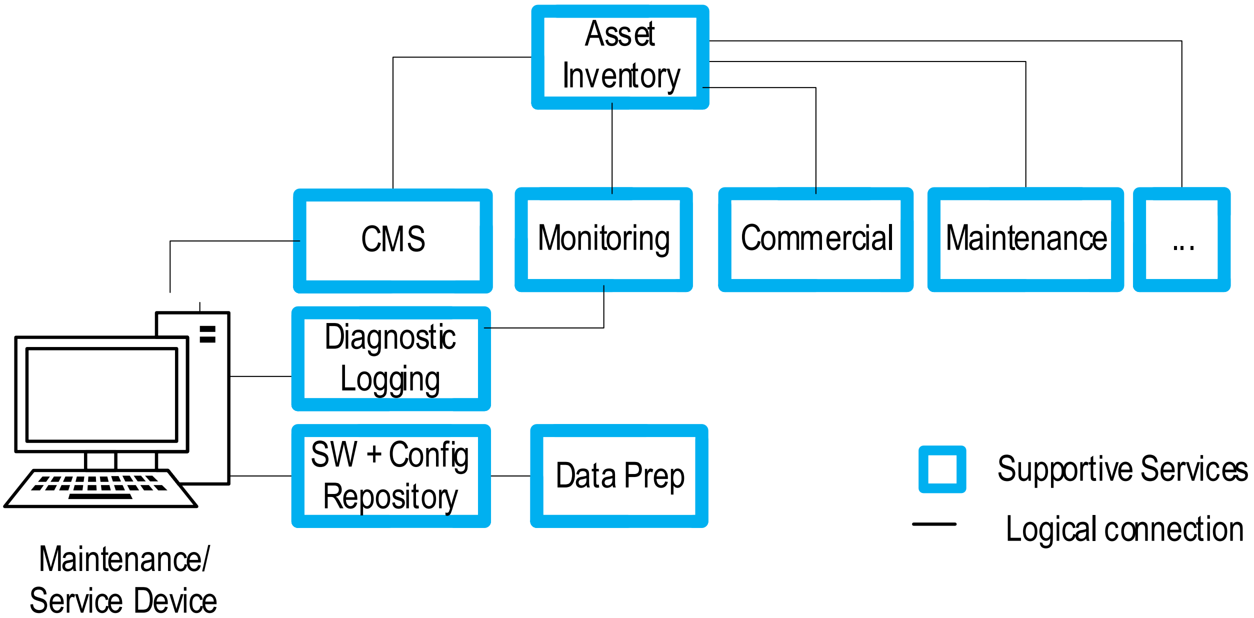

Figure 7: Supportive Services overview

5.3.1 Asset Management

The asset inventory is part of the asset management process. The asset management is used to track the lifecycle of all hardware and software assets. The assets managed include all assets relevant within the vehicle architecture and not only the security related assets. It tracks the data of assets beginning with the interface from the procurement management, ending with the decommissioning.

This service is a non-technical service using available technical systems of a Railway Undertaking and is interconnected with commercial processes, including supply chain and procurement processes.

The asset management contains amongst others:

- Asset Inventory,
- Configuration Management System (CMS),
- Maintenance aspects,

- Commercial aspects.

For use within OCORA, the CMS is relevant for the Software (configuration and software) management process. The CMS manages the software and configuration of the assets in the context of a desired overall state. This service is sometimes referred as Configuration Management Database (CMDB). It must provide a versioning system which records and provides the configuration used by the assets. The CMS does not store software or configurations. The software and configuration are stored in the SW+Config Repository.

The CMS orchestrates configuration updates using the SW+Config Repository service to deploy software files and configuration.

A maintenance and diagnostic device that has the right to update the onboard systems, shall support this task by performing a lookup for the software and configuration version defined in the CMS. Afterwards it is requesting the corresponding software and configuration from the SW+Config Repository. This software and configuration are then deployed to the asset. This service is a technical service interconnected to the life-cycle-management of the asset and the system, as well as with data preparation procedures. This service supports keeping the overall system in a certified state. The process is displayed in Figure 8.

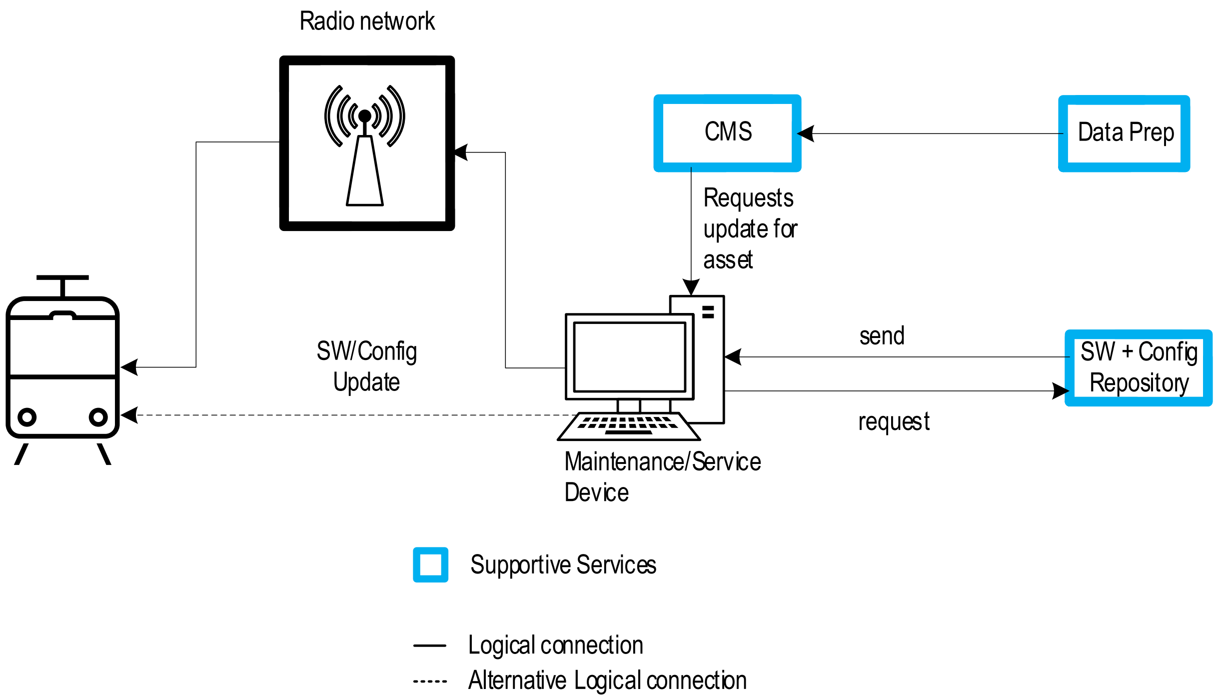

Figure 8: Supportive Services SW/Config Update

Asset inventory must include attributes to each asset giving indication on their position and function in the logical architecture (e.g., to be used for risk inheritance during risk management process) and physical architecture (e.g., to be used for updates, retrofit efforts)

The asset inventory shall provide the following connectivity and support interaction:

- Interacts with Life-Cycle Managers
- Interacts with maintenance personnel (maintenance, replacement)
- Interacts with build projects (import/create assets to be managed)
- Interacts with IAM (basic data for identity, decommissioning of asset)
- Supports maintenance activities
- Provides technical, commercial and supply chain data based on authentication and authorization based on IAM service
- documents physical (e.g., location) and high-level logical (e.g., EIL area) context of asset

- Provide Configuration Management System (CMS) orchestrating software and configuration changes ensuring compliance with safety regulation/certificates
- The Configuration Management System interacts with processes/systems supporting change
- The Configuration Management System interacts with the MDM

The Configuration Management System uses the Software & Configuration Repository service

5.3.2 Assumption on Maintenance

During the process of the review presented in Chapter 4.2.3 several assumptions on the maintenance and on-board security services were necessary. These services are currently not defined in the OCORA architecture or specifications. The assumptions provide a basis for the future work of upcoming releases in the TWS06 Security. They do not represent any specified solution yet.

Figure 9 shows the distribution across the onboard and infrastructure side systems. The Onboard Security Services (OSS) are connected to the internal network and to the infrastructure via the ECN-Security Gateway. The SSS-Trackside (SSS-TS) are located at the infrastructure of the RU and connected to supporting (security) services like the OCS-RU and the SOC (yellow). Arrows in the figure indicate if the specific service is the main data source or if it is a mirror of a subset of the data (Destination).

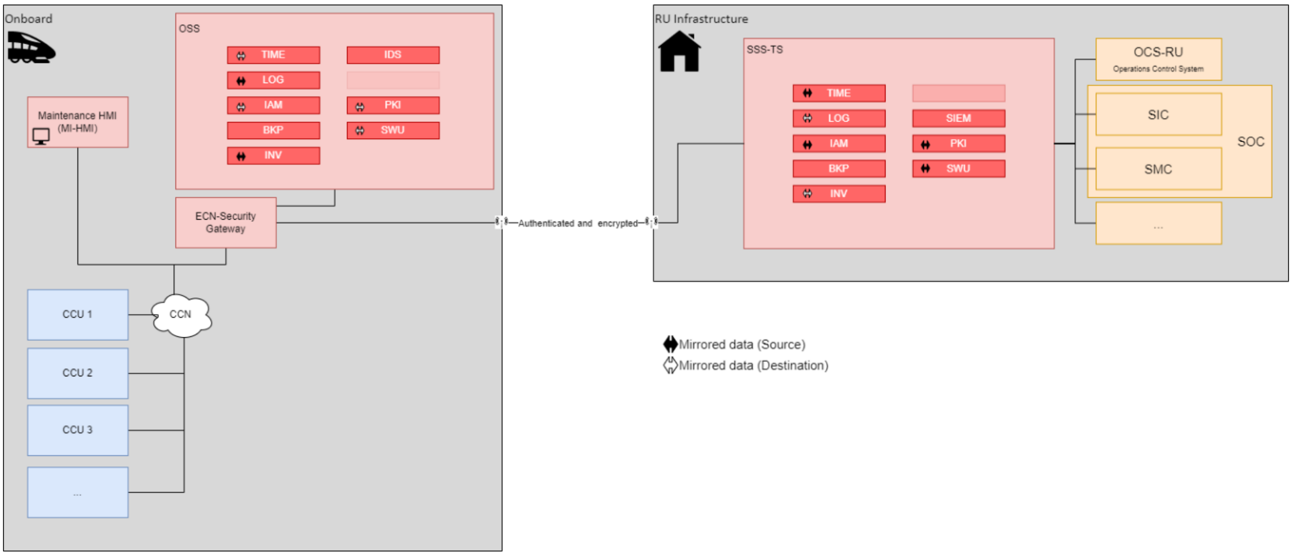

Figure 9: OSS and SSS-TS

Following services are defined in the OSS and SSS-TS:

- TIME: Time source syncing the local OSS TIME to the SSS-TS TIME
- IDS: OSS side Intrusion Detection System
- LOG: Logging service uploading the local OSS data to the SSS-TS
- SIEM: Security Incident and Event Management on SSS-TS using the data provided by LOG
- IAM: Identity and Access Management provided by SSS-TS which is mirrored to the OSS for local use.
- PKI: Public Key Infrastructure which is managed centrally in the SSS-TS. Parts of the PKI might be mirrored to the OSS (e.g., CRLs)
- BKP: Local and infrastructure side backup. Local backup might contain e.g., logging information and previously used software and configuration files for rollback. Infrastructure side might include software and configuration files, logging data and other backups of other services.
- SWU: Software and configuration repository available at SSS-TS. Update files could be transferred to the OSS SWU and saved locally until they are applied.
- INV: OSS side inventory of all components as well as software/configuration versions which is transferred to the SSS-TS.

In Figure 10 the connection from the MT to the OBU is shown. The figure describes how a software- or configuration change must be performed to ensure complete coverage of the requirement given by the applied standards.

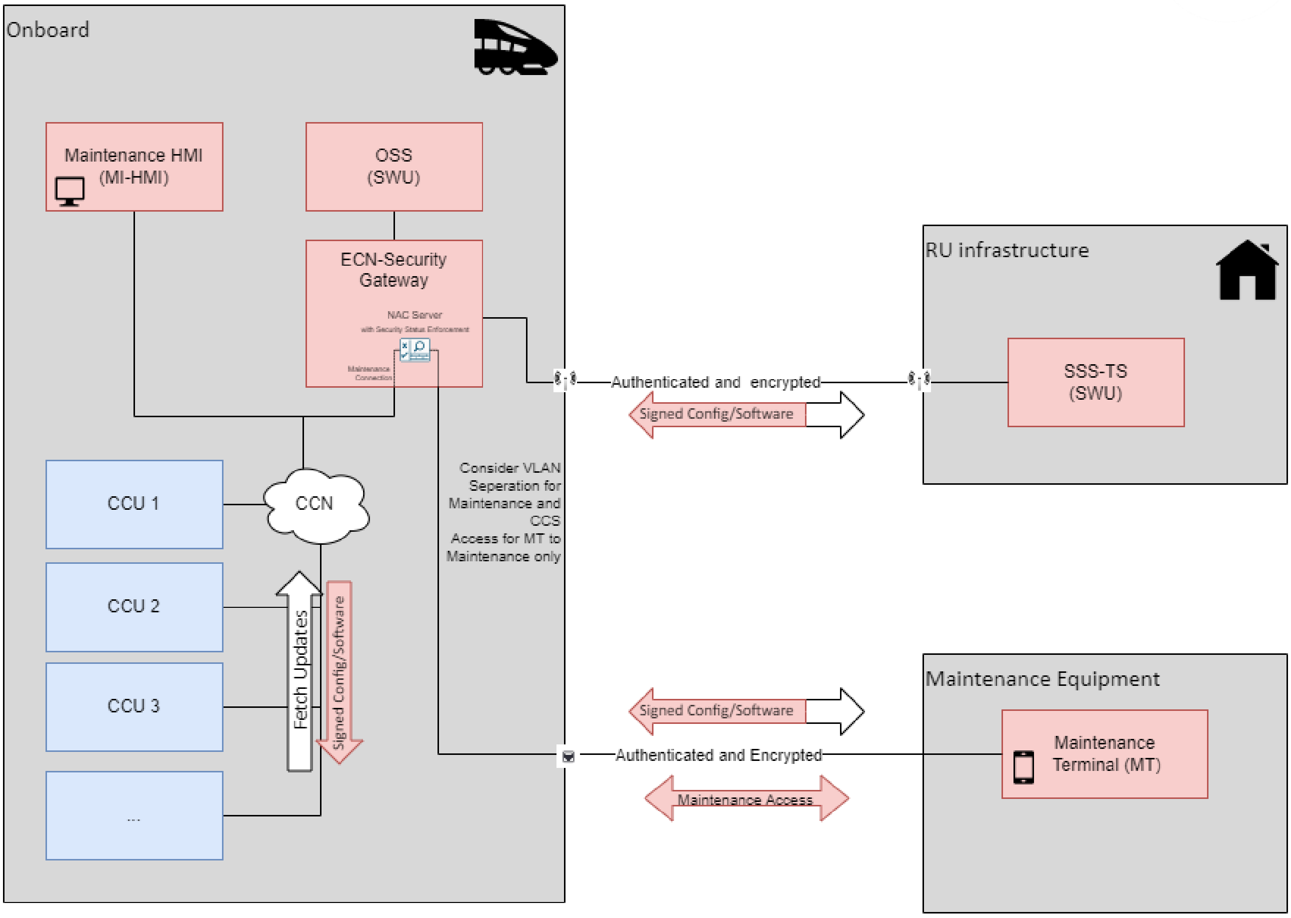

Figure 10: Assumptions on Maintenance

In the following the different update scenarios are described using the approach shown in the figure above.

Direct Maintenance Connection via MT

The MT establishes a connection to a component (e.g., EVC) via the ECN-Security Gateway and using a separated VLAN. After successfully establishing a connection and reaching the destination component only signed (software or configuration) files are allowed to be transferred to the component.

Software and Configuration Update:

SSS-TS Update

The SSS-TS establishes a connection to the ECN-Security gateway. A direct connection from the SSS-TS to another component of the onboard system must be prohibited. Files are allowed to be transferred to the OSS and the rollout of the change can be planed or executed.

MT Update:

The MT establishes a connection to the ECN-Security gateway. A direct connection from the MT to another component of the onboard system must be prohibited. Files are allowed to be transferred to the OSS and the rollout of the change can be planed or executed.

6 Annex

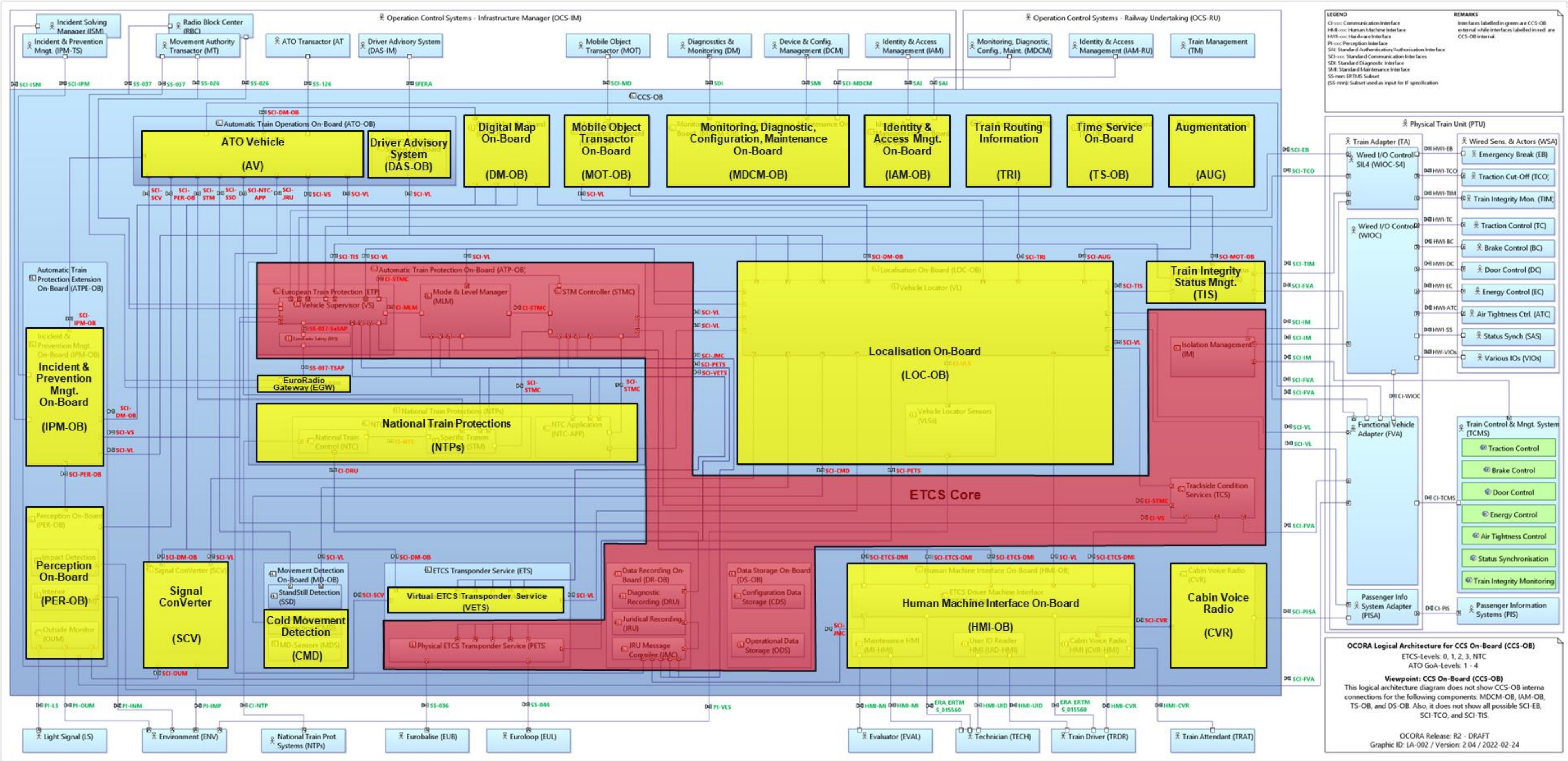

Figure 11: Building Blocks

OCORA - Assessment of the Protection Requirements

Assessment of the protection requirements of the logical architecture of OCORA

OCORA TWS 06

Version 1.0

Assumptions	Comment
Non repudation is set to middle if health damage is (very) high in other APR categories. It is set to middle as juridical consequences and nation wide reporting can be expected if the cause of an accident can not be identified.	
Availability is always connected to the evaluation of the assessed interface.	
Availability is set to low, if a non-availability is not linked to any safety critical reaction and only one train can be affected.	
Availability is set to high or very high, if a non-availability is linked to a safety critical reaction, e.g. the Emergenc break.	
Availability is set to high, if a non-availability of one in one train is linked to a fleet fail.	

Assessment of the protection requirements

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hum Mac
1	SCI-VL	HMI-OB	ETCS-DMI	LOC-OB	VL	External	<-	Not relevant	Very High	Low	Middle	Not relevant
2	SCI-TCS	HMI-OB	ETCS-DMI	TCS	TCS	External	<-	Not relevant	Middle	Middle	Middle	Not relevant
3	SCI-ETCS-DMI	HMI-OB	ETCS-DMI	ATP-OB	STMC	External	<-	Not relevant	Low	Low	Low	Not relevant
4	SCI-ETCS-DMI	HMI-OB	ETCS-DMI	ATP-OB	MLM	External	<->	Not relevant	Very High	Low	Middle	Not relevant
5	SCI-ETCS-DMI	HMI-OB	ETCS-DMI	ATP-OB	VS	External	<->	Not relevant	Very High	Low	Middle	Not relevant
6	SCI-JMC	HMI-OB	ETCS-DMI	DR-OB	JMC	External	->	Not relevant	Middle	Middle	Middle	Not relevant
7	SCI-CVR	HMI-OB	CVR-HMI	CVR	CVR	External	->	Not relevant	Very High	Low	Middle	Not relevant
8	-	HMI-OB	MI-HMI	Human	EVAL	External	<->	Not relevant	Low	Low	Low	
9	-	HMI-OB	MI-HMI	Human	TECH	External	<->	Not relevant	Very High	Low	Middle	Very High
10	-	HMI-OB	ETCS-DMI	Human	TECH	External	<->	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
11	-	HMI-OB	UID-HMI	Human	TECH	External	<->	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
12	-	HMI-OB	UID-HMI	Human	TRDR	External	<->	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
13	-	HMI-OB	ETCS-DMI	Human	TRDR	External	<->	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
14	-	HMI-OB	CVR-HMI	Human	TRDR	External	<->	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
15	-	HMI-OB	CVR-HMI	Human	TRAT	External	<->	Not relevant	Middle	Low	Low	Not relevant
16	SCI-VL	LOC-OB	VL	TCS	TCS	External	->	Not relevant	Middle	Middle	Middle	Not relevant
17	HMI	LOC-OB	VL	TA	PISA	External	->	Not relevant	Low	Low	Low	Not relevant
18	-	LOC-OB	VL	TA	FVA	External	->					
19	SCI-TIS	LOC-OB	VL	TIS	TIS	External	<-	Not relevant	Very High	High	Middle	Not relevant
20	SCI-AUG	LOC-OB	VL	AUG	AUG	External	<-					

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hu Ma
21	SCI-TRI	LOC-OB	VL	TRI	TRI	External	<-					
22	SCI-VL	LOC-OB	VL	MOT-OB	MOT-OB	External	->					
23	SCI-DM-OB	LOC-OB	VL	DM-OB	DM-OB	External	<-	Not relevant	Very High	High	Middle	Not relevant
24	SCI-VL	LOC-OB	VL	ATO-OB	DAS-OB	External	->	Not relevant	Low	Low	Low	Not relevant
25	SCI-VL	LOC-OB	VL	ATO-OB	AV	External	->	Not relevant	Middle	Low	Low	Not relevant
26	SCI-VL	LOC-OB	VL	ATPE-OB	IPM-OB	External	->	Not relevant	Low	Low	Not relevant	Not relevant
27	SCI-VL	LOC-OB	VL	ATP-OB	MLM	External	->	Not relevant	Very High	High	Middle	Not relevant
28	SCI-VL	LOC-OB	VL	ATP-OB	VS	External	->	Not relevant	Very High	High	Middle	Not relevant
29	SCI-VL	LOC-OB	VL	ATP-OB	STMC	External	->	Not relevant	Very High	High	Middle	Not relevant
30	SCI-VL	LOC-OB	VL	ATP-OB	NTC-APP	External	->	Not relevant	Very High	High	Middle	Not relevant
31	SCI-VL	LOC-OB	VL	SCV	SCV	External	->					
32	SCI-VL	LOC-OB	VL	MD-OB	SSD	External	->	Not relevant	High	Low	Middle	Not relevant
33	SCI-CMD	LOC-OB	VL	MD-OB	CMD	External	<-					
34	SCI-VL	LOC-OB	VL	ETS	VETS	External	->	Not relevant	Very High	Low	Middle	Not relevant
35	SCI-PETS	LOC-OB	VL	ETS	PETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
36	CI-VLS	LOC-OB	VL	LOC-OB	VLSs	Internal	<-	Not relevant	Very High	Low	Middle	Not relevant
37	-	LOC-OB	VLSs	ENV	ENV	External	<-					
38	SCI-TMC	ATP-OB	STMC	ATP-OB	NTC-APP	External	<->	Not relevant	Very High	Low	Middle	Not relevant
39	SCI-JMC	ATP-OB	STMC	DR-OB	JMC	Internal	->	Not relevant	Middle	Middle	Middle	Not relevant
40	SCI-JMC	ATP-OB	MLM	DR-OB	JMC	Internal	->	Not relevant	Middle	Middle	Middle	Not relevant
41	SCI-JMC	ATP-OB	VS	DR-OB	JMC	Internal	->	Not relevant	Middle	Middle	Middle	Not relevant

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hum Mac
42	SCI-PETS	ATP-OB	STMC	ETS	PETS	Internal	<-	Not relevant	Very High	Low	Middle	Not relevant
43	SCI-PETS	ATP-OB	MLM	ETS	PETS	Internal	<-	Not relevant	Very High	Low	Middle	Not relevant
44	SCI-PETS	ATP-OB	NTC-APP	ETS	PETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
45	SCI-PETS	ATP-OB	STM	ETS	PETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
46	SCI-PETS	ATP-OB	VS	ETS	PETS	Internal	<-	Not relevant	Very High	Low	Middle	Not relevant
47	SCI-VETS	ATP-OB	NTC-APP	ETS	VETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
48	SCI-VETS	ATP-OB	STMC	ETS	VETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
49	SCI-VETS	ATP-OB	STM	ETS	VETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
50	SCI-VETS	ATP-OB	MLM	ETS	VETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
51	SCI-VETS	ATP-OB	VS	ETS	VETS	External	<-	Not relevant	Very High	Low	Middle	Not relevant
52	SCI-STMC	ATP-OB	STMC	ATP-OB	STM	External	<->	Not relevant	Very High	Low	Middle	Not relevant
53	CI-STMC	ATP-OB	STMC	ATP-OB	MLM	Internal	<->	Not relevant	Very High	Low	Middle	Not relevant
54	CI-STMC	ATP-OB	STMC	ATP-OB	VS	Internal	<->	Not relevant	Very High	Low	Middle	Not relevant
55	CI-MLM	ATP-OB	MLM	ATP-OB	VS	Internal	<->	Not relevant	Very High	Low	Middle	Not relevant
56	SCI-TIS	ATP-OB	VS	TIS	TIS	External	<-	Not relevant	Very High	High	Middle	Not relevant
57	-	ATP-OB	VS	TA	FVA	External	<->	Not relevant	Middle	Low	Low	Not relevant
58	SCI-VS	ATP-OB	VS	ATO-OB	AV	External	<-	Not relevant	Low	Low	Not relevant	Not relevant
59	-	ATP-OB	VS	TA	WIOC-S4	External	->	Not relevant	Very High	Low	Middle	Not relevant
60	-	ATP-OB	VS	TA	WIOC	External	->	Not relevant	High	Low	Middle	Not relevant
61	-	ATP-OB	VS	OCS-IM	RBC	External	<->	Not relevant	Very High	Low	Middle	Not relevant
62	-	ATP-OB	VS	OCS-IM	MT	External	<->	Not relevant	Very High	Low	Middle	Not relevant

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hu Mac
63	SCI-VS	ATP-OB	VS	ATPE-OB	IPM-OB	External	<-	Not relevant	Very High	Low	Middle	Not relevant
64	SS-037-SaSAP	ATP-OB	VS	ATP-OB	ERS	Internal	<->	Not relevant	Very High	Low	Middle	Not relevant
65	SS-037-TSAP	ATP-OB	EGW	ATP-OB	ERS	External	<->	Not relevant	Very High	Low	Middle	Not relevant
66	-	ATP-OB	EGW	OCS-IM	MT	External	<->	Not relevant	Very High	Low	Middle	Not relevant
67	-	ATP-OB	EGW	OCS-IM	RBC	External	<->	Not relevant	Very High	Low	Middle	Not relevant
68	SCI-NTC-APP	ATP-OB	NTC-APP	ATO-OB	AV	External	<-	Not relevant	Middle	Low	Low	Not relevant
69	SCI-STM	ATP-OB	STM	ATO-OB	AV	External	<-	Not relevant	Middle	Low	Low	Not relevant
70	SCI-NTC	ATP-OB	STM	ATP-OB	NTC	Internal	<->	Not relevant	Very High	Low	Middle	Not relevant
71	-	ATP-OB	NTC	NTPs	NTPs	Internal	<-					
72	SCI-DRU	ATP-OB	NTC	DR-OB	DRU	External	->	Not relevant	Low	Low	Low	Not relevant
73	SCI-JRU	ATO-OB	AV	DR-OB	JMC	External	->	Not relevant	Low	Low	Low	Not relevant
74	SCI-SSD	ATO-OB	AV	MD-OB	SSD	External	<-	Not relevant	Middle	Low	Low	Not relevant
75	SCI-PER-OB	ATO-OB	AV	PER-OB	PER-OB	External	<-	Not relevant	Low	Low	Low	Not relevant
76	SCI-SCV	ATO-OB	AV	SCV	SCV	External	<-	Not relevant	Low	Low	Low	Not relevant
77	SCI-IPM-OB	ATO-OB	AV	ATPE-OB	IPM-OB	External	<-	Not relevant	Low	Low	Low	Not relevant
78	-	ATO-OB	AV	TA	FVA	External	<->	Not relevant	Low	Low	Low	Not relevant
79	SCI-DM-OB	ATO-OB	AV	DM-OB	DM-OB	External	<-	Not relevant	Low	Low	Low	Not relevant
80	-	ATO-OB	AV	OCS-IM	AT	External	<->	Not relevant	Low	Low	Low	Not relevant
81	-	ATO-OB	DAS-OB	OCS-IM	DAS-IM	External	<->	Not relevant	Low	Low	Low	Not relevant
82	SCI-DM-OB	DM-OB	DM-OB	ETS	VETS	External	->	Not relevant	Very High	Low	Middle	Not relevant
83	SCI-DM-OB	DM-OB	DM-OB	SCV	SCV	External	->	Not relevant	Very High	Low	Middle	Not relevant

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hum Mac
84	SCI-DM-OB	DM-OB	DM-OB	ATPE-OB	IPM-OB	External	->	Not relevant	Very High	Low	Middle	Not relevant
85	-	ATPE-OB	IPM-OB	OCS-IM	IPM-TS	External	<->	Not relevant	Low	Low	Low	Low
86	-	ATPE-OB	IPM-OB	OCS-IM	ISM	External	<->	Not relevant	Low	Low	Low	Low
87	SCI-PER-OB	ATPE-OB	IPM-OB	ATPE-OB	PER-OB	External	<-	Not relevant	Very High	Low	Middle	Not relevant
88	-	ATPE-OB	IMP	ENV	ENV	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
89	-	ATPE-OB	INM	ENV	ENV	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
90	CI-OUM	ATPE-OB	OUM	SCV	SCV	External	->					
91	-	ATPE-OB	PER-OB	TA	FVA	External	<-	Not relevant	Low	Low	Low	Not relevant
92	-	ATPE-OB	OUM	ENV	ENV	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
93	-	ATPE-OB	OUM	LS	LS	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
94	-	ETS	PETS	EUB	EUB	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
95	-	ETS	PETS	EUL	EUL	External	<-	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
96	SCI-SCV	SCV	SCV	ETS	VETS	External	->	Not relevant	Very High	Low	Middle	Not relevant
97	-	DR-OB	JMC	DR-OB	JRU	Internal	->	Not relevant	Middle	Middle	Middle	Not relevant
98	SCI-STMC	ATP-OB	STMC	TCS	TCS	Internal	->	Not relevant	Middle	Middle	Middle	Not relevant
99	-	CVR	CVR	TA	PISA	External	<->	Not relevant	Very High	Low	Middle	Not relevant
100	-	TCS	TCS	TA	FVA	External	->	Not relevant	Middle	Middle	Middle	Not relevant
101	-	IM	IM	TCMS	TCMS	External	->					
102	-	IM	IM	TA	WIOC	External	->					
103	-	IM	IM	TA	WIOC-S4	External	->					
104	-	TIS	TIS	TA	FVA	External	<-	Not relevant	Very High	Low	Middle	Not relevant

Interface ID	Interface Name	Component Group A	Component A	Component Group B	Component B / Personell	Building Block Connection	Direction	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Hu Mac
105	-	TIS	TIS	TA	WIOC-S4	External	<-	Not relevant	Very High	Low	Middle	Not relevant
106	SCI-MOT-OB	TIS	TIS	MOT-OB	MOT-OB	External	<-					
107	-	IAM-OB	IAM-OB	OCS-RU	IAM-RU	External	<->					
108	-	IAM-OB	IAM-OB	OCS-IM	IAM	External	<->					
109	-	MDCM-OB	MDCM-OB	OCS-RU	MDCM	External	<->	Very High	Very High	Low	Middle	Very High
110	-	MDCM-OB	MDCM-OB	OCS-IM	DCM	External	<-	Very High	Very High	Low	Middle	Very High
111	-	MDCM-OB	MDCM-OB	OCS-IM	DM	External	->	Very High	Very High	Low	Middle	Very High
112	-	MOT-OB	MOT-OB	MOT	MOT	External	<->	Not relevant	Very High	Low	Middle	Not relevant
113	-	LOC-OB	VL	TA	PISA	External	->	Not relevant	Low	Low	Low	Not relevant

Definitions:	*privacy (e.g. EU DSGV) is a combination of Confidentialiy (information can not be read by anyone), Integrity (not changed) and Authenticy (the right person(s) have access) *The measures are not taken from the IEC 62443-3-3 and -4-2 since in this state of the CENELEC and security life cycle process to zones and conduits, and thus no SL level can be defined. *For juridical prossecution availabilit of data and non repudiation are in direct connection. *chapter availability focusses on the operational availability, what means that the relevant information or systems shall be "permanently" available to ensure operation. * encryption: encrypt then sign/mac; when combining integrity and confidentiality: sign payload then encrypt then sign/mac * encryption and signing: the respecitve endpoints or consumers are authenticated for beeing the correct encryption endpoint or the correct signer * authenticty in machine-machine situation is part of confidentiality and/or integrity as both endpoints must authenticate to the other

		APR highes requirement from **Confidentiality**				
		not relevant	low	medium	high	very high
component	**data (information) at rest and software**	no measure	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening	encrypted data storage with min. AES 256, procesual measures and physical protection, basic hardening	encrypted data storage with min. AES 256, procesual measures and physical protection, basic hardening
	SW 2 SW comm. (pure internal)	no measure	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening	the developper must consider security with respect of implementing SL-T and expected attacker category.	the developper must consider security with respect of implementing SL-T and expected attacker category.
Connection type	**internal network**	no measure	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication
	wired (external)	no measure	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication
	radio (external)	no measure	AES 128 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication	min. AES 256 encryption end to end with endpoint authentication

		APR highes requirement from **Integrity**				
		not relevant	low	medium	high	very high
component	**data (information) at rest and software**	no measure	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening	signed data storage (e.g. SHA256, Curve25519), physical protection, basic hardening	signed data storage (e.g. SHA512, Curve25519), physical protection, basic hardening
	SW 2 SW comm. (pure internal)	no measure	procesual measures and physical protection, basic hardening	procesual measures and physical protection, basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA512, Curve25519), basic hardening
Connection type	**internal network**	no measure	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening, monitoring/detection of malware (SIEM) with central logging	strong signed data (e.g. SHA512, Curve25519), basic hardening, or SHA256 and encrypted traffic min. AES 256, monitoring/detection of malware (SIEM) with central logging
	wired (external)	no measure	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening, monitoring/detection of malware (SIEM) with central logging	strong signed data (e.g. SHA512, Curve25519), basic hardening, or SHA256 and encrypted traffic min. AES 256, monitoring/detection of malware (SIEM) with central logging
	radio (external)	no measure	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening	signed data (e.g. SHA256, Curve25519), basic hardening, monitoring/detection of malware (SIEM) with central logging	strong signed data (e.g. SHA512, Curve25519), basic hardening, or SHA256 and encrypted traffic min. AES 256, monitoring/detection of malware (SIEM) with central logging

		APR highes requirement from **Availability**				
		not relevant	low	medium	high	very high
component	**data (information) at rest and software**	no measure	protect component availability low (no standby); automated back-up, role-back strategy	protect component availability medium (cold-standby); automated back-up, role-back strategy	protect component availability high (redundancy, hot-standby); automated back-up, 3-2-1 rule (3 copies, 2 media types, 1 external storage (other location, cloud, ..), role-back strategy, desaster recovery process	protect component availability (parallel operation); automated back-up, 3-2-1 rule (3 copies, 2 media types, 1 external storage (other location, cloud, ..), role-back strategy, desaster recovery process
	SW 2 SW comm. (pure internal)	no measure	secure coding; resource availability	secure coding; resource availability	secure coding; resource availability (resource management)	secure coding; resource availability (resource management)
Connection type	**internal network**	no measure	protect node	protect node and/or edge redundancy, network-style setup, routing	protect node and edge redundancy, network-style setup, routing; components very reliable and high available	protect node and edge redundancy, network-style setup, routing; components very reliable and very high available

	wired (external)	no measure	protect node	protect node and/or edge redundancy, network-style setup, routing	protect node and edge redundancy, network-style setup, routing; components very reliable and high available	protect node and edge redundancy, network-style setup, routing; components very reliable and very high available
	radio (external)	no measure	one network, simple design, basic availability concepts	two radio networks, one or more core networks	two radio networks with own core or high availability one-network-design; with automated detection of availability load handling and "switching" between networks; or combination radio and wired networks	multi-network, multi-source, multi-operator (not service provider, operator!) with automated detection of availability load handling and "switching" between networks + cabled network or "wire breackage proof" required (process reciliency to connection interruption)

		APR highes requirement from **Non Repudiation**				
		not relevant	low	medium	high	very high
component	**data (information) at rest and software**	no measure	changing information is directly transferred to a protected logging capability and saved on the component for a predefined timespan if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	changing information is directly transferred to a independent logging facility and saved on the device for a predefined timespan in case of communication interruption (take time for connection reastablishment/repair into account); integrity of local log is protected with a signature similar to integrity level "high"; if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	changing information is directly transferred to a independent logging facility and saved on the device for a predefined timespan in case of communication interruption (take time for connection reastablishment/repair into account); integrity of local log is protected with level "high"; authenticity is protected with level "high" (authenticity of devices/service must be protected with similar measures); availability is protected with level at least "high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	changing information is directly transferred to a independent logging facility and saved on the device for a predefined timespan in case of communication interruption (take time for connection reastablishment/repair into account); integrity of local log is protected with level "very high"; authenticity is protected with level "very high" (authenticity of devices/service must be protected with similar measures); availability is protected with level at least "very high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"
	SW 2 SW comm. (pure internal)	no measure	log information integrity protected with integrity level "low" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	log information is protected with integrity level "medium" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	local/process log information is protected with integrity level "high"; information is written to local storage and processed as "data at rest" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	local/process log information is protected with integrity level "very high"; information is written to local storage and processed as "data at rest" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"
Connection type	**internal network**	no measure	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "low" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "medium" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "very high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"
	wired (external)	no measure	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "low" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "medium" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "very high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"
	radio (external)	no measure	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "low" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "medium" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"	the fact that this information is transfered is logged (time stamp and source/target) at both processual endpoints of the transfer. This log must be protected like component data at rest with integrity and availability similar as "very high" if logged data contain privacy-related information the log has to be protected with meaures similar to confidentiality "high"

		APR highes requirement from **Authenticity** (only				

		not relevant	low	medium	high	very high
component	**data (information) at rest and software**	not applicable	not applicable	not applicable	not applicable	not applicable
	SW 2 SW comm. (pure internal)	not applicable	not applicable	not applicable	not applicable	not applicable
	HMI process	no measure	username, no or weak password; roles for authorization	username, strong password; roles for authorization	username, multi-factor authentication; roles for authorization	username, multi-factor authentication; roles for authorization
Connection type	**internal network**	not applicable	not applicable	not applicable	not applicable	not applicable
	wired (external)	not applicable	not applicable	not applicable	not applicable	not applicable
	radio (external)	not applicable	not applicable	not applicable	not applicable	not applicable

Max per Component

Component	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
AT	Not relevant	Low	Low	Low	Not relevant
AUG	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
AV	Not relevant	Middle	Low	Low	Not relevant
CMD	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
CVR	Not relevant	Very High	Low	Middle	Not relevant
CVR-HMI	Not relevant	Very High	Low	Middle	Not relevant
DAS-IM	Not relevant	Low	Low	Low	Not relevant
DAS-OB	Not relevant	Low	Low	Low	Not relevant
DCM	Very High	Very High	Low	Middle	Very High
DM	Very High	Very High	Low	Middle	Very High
DM-OB	Not relevant	Very High	High	Middle	Not relevant
DRU	Not relevant	Low	Low	Low	Not relevant
EGW	Not relevant	Very High	Low	Middle	Not relevant
ENV	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
ERS	Not relevant	Very High	Low	Middle	Not relevant
ETCS-DMI	Not relevant	Very High	Middle	Middle	Not relevant
EUB	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
EUL	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
EVAL	Not relevant	Low	Low	Low	Not relevant
FVA	Not relevant	Very High	Middle	Middle	Not relevant
IAM	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IAM-OB	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IAM-RU	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IM	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IMP	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
INM	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
IPM-OB	Not relevant	Very High	Low	Middle	Low
IPM-TS	Not relevant	Low	Low	Low	Low
ISM	Not relevant	Low	Low	Low	Low
JMC	Not relevant	Middle	Middle	Middle	Not relevant
JRU	Not relevant	Middle	Middle	Middle	Not relevant
LS	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
MDCM	Very High	Very High	Low	Middle	Very High
MDCM-OB	Very High	Very High	Low	Middle	Very High
MI-HMI	Not relevant	Very High	Low	Middle	Very High
MLM	Not relevant	Very High	High	Middle	Not relevant
MOT	Not relevant	Very High	Low	Middle	Not relevant
MOT-OB	Not relevant	Very High	Low	Middle	Not relevant
MT	Not relevant	Very High	Low	Middle	Not relevant
NTC	Not relevant	Very High	Low	Middle	Not relevant
NTC-APP	Not relevant	Very High	High	Middle	Not relevant
NTPs	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
OUM	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
PER-OB	Not relevant	Very High	Low	Middle	Not relevant
PETS	Not relevant	Very High	Low	Middle	Not relevant

Max per Building Block

Component	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
External	Very High	Very High	Low	Middle	Very High
AUG	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
AV	Not relevant	Middle	Low	Low	Not relevant
CMD	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
CVR	Not relevant	Very High	Low	Middle	Not relevant
HMI-OB	Not relevant	Very High	Middle	Middle	Very High
DAS-OB	Not relevant	Low	Low	Low	Not relevant
DM-OB	Not relevant	Very High	High	Middle	Not relevant
ETCS Core	Not relevant	Very High	High	Middle	Not relevant
EGW	Not relevant	Very High	Low	Middle	Not relevant
PTU-External	Not relevant	Very High	Middle	Middle	Not relevant
IAM-OB	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
PER-OB	Not relevant	Very High	Low	Middle	Not relevant
IPM-OB	Not relevant	Very High	Low	Middle	Low
MDCM-OB	Very High	Very High	Low	Middle	Very High
MOT-OB	Not relevant	Very High	Low	Middle	Not relevant
NTPs	Not relevant	Very High	High	Middle	Not relevant
SCV	Not relevant	Very High	Low	Middle	Not relevant
n/a	Not relevant	High	Low	Middle	Not relevant
TIS	Not relevant	Very High	High	Middle	Not relevant
TRI	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
VETS	Not relevant	Very High	Low	Middle	Not relevant
LOC-OB	Not relevant	Very High	High	Middle	Not relevant

Component	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)
PISA	Not relevant	Very High	Low	Middle	Not relevant
RBC	Not relevant	Very High	Low	Middle	Not relevant
SCV	Not relevant	Very High	Low	Middle	Not relevant
SSD	Not relevant	High	Low	Middle	Not relevant
STM	Not relevant	Very High	Low	Middle	Not relevant
STMC	Not relevant	Very High	High	Middle	Not relevant
TCMS	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
TCS	Not relevant	Middle	Middle	Middle	Not relevant
TECH	Not relevant	Very High	Low	Middle	Very High
TIS	Not relevant	Very High	High	Middle	Not relevant
TRAT	Not relevant	Middle	Low	Low	Not relevant
TRDR	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
TRI	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
UID-HMI	Not relevant	Not relevant	Not relevant	Not relevant	Not relevant
VETS	Not relevant	Very High	Low	Middle	Not relevant
VL	Not relevant	Very High	High	Middle	Not relevant
VLSs	Not relevant	Very High	Low	Middle	Not relevant
VS	Not relevant	Very High	High	Middle	Not relevant
WIOC	Not relevant	High	Low	Middle	Not relevant
WIOC-S4	Not relevant	Very High	Low	Middle	Not relevant

Component	Confidentiality	Integrity	Availability	Non-Repudiation	Authenticity (only Human-Machine-Interaction)