OCORA

Open CCS On-board Reference Architecture

Cyber Security – Overview
Beta Release

Document ID: OCORA-40-008-Beta

Version: 1.10

Date: 30.06.2020

Status: final

Revision history

Version	Change Description	Name (Initials)	Date of change
1.00	First version for formal review	RMe	2020-05-29
1.01	Update of requirements. Risk analyses and requirements process added to the main workstream activities. Comments from formal review addressed: - Hans Willemsen - Quentin Rivette - Urs Fuchser - Olaf Zanger	RMe	2020-06-17
1.02	Minor change (chapter 3.1)	RMe	2020-06-22
1.1	Final for Beta Release	RM	2020-06-30

Table of contents

Table of tables

Table of figures

References

The following references are used in this document:

[1] OCORA-10-001-Beta – Release Notes

[2] OCORA-30-001-Beta – Introduction to OCORA

[3] OCORA-30-002-Beta – Problem Statements

[4] OCORA-40-001-Beta – System Architecture

[5] OCORA-40-007-Beta – Set of Requirements

[6] OCORA-90-002-Beta – Glossary

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

[8] prTS 50701 Railway application - Cybersecurity

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

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

1 Management Summary

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

Therefore, OCORA is required to also consider security aspects of CCS on-board solutions. In European cooperation security experts from DB, NS, SBB, SNCF will develop a set of well-defined security requirements as an addition for the OCORA release 1.0 requirement catalog. This will be achieved by developing a process to define new security requirements and by revisions of already existing ones through workshops.

The two main objectives of the OCORA security workstream is the creation of security requirements as an addition for the OCORA requirement catalog and that (cyber-) security thoughts get integrated in the OCORA architecture like zoning, principles, and levels. The workstream will also include opinions and results from other security work groups.

With the gamma release of OCORA a revised “OCORA Cyber – Security Overview” document and an updated set of requirements will be published. With the OCORA release 1.0 the final document and set of security requirements will be available.

2 Introduction

2.1 Document context and purpose

This document is published as part of the OCORA Beta release, together with the documents listed in the release notes [1]. It is the first release of this document and it is still in a preliminary state.

Subsequent releases of this document (gamma, etc.) and topic specific documentation will be developed in a modular and iterative approach, evolving within the progress of the OCORA collaboration.

This document aims to provide the reader with:

- reasons why (cyber-) security needs to be treaded and on an international level
- an evolution of security requirements for on-board CCS solutions
- an approach on how to define the security requirements
- a set of on-board CCS security requirements

2.2 Why should I read this document?

This document addresses experts in the railway security domain and to any other person, interested in security requirements for on-board CCS solutions. The reader will be able to provide feedback to the authors and can, therefore, engage in shaping OCORA security requirements.

Prior to reading this document, it is recommended to study the Release Notes [1], the Introduction to OCORA [2] and the Problem Statements [3]. The reader should also be aware of the Glossary [6].

2.3 System under consideration

The system under consideration is the CCS onboard application platform reference architecture designed by the work group OCORA outlined in Figure 1 (green boarders).

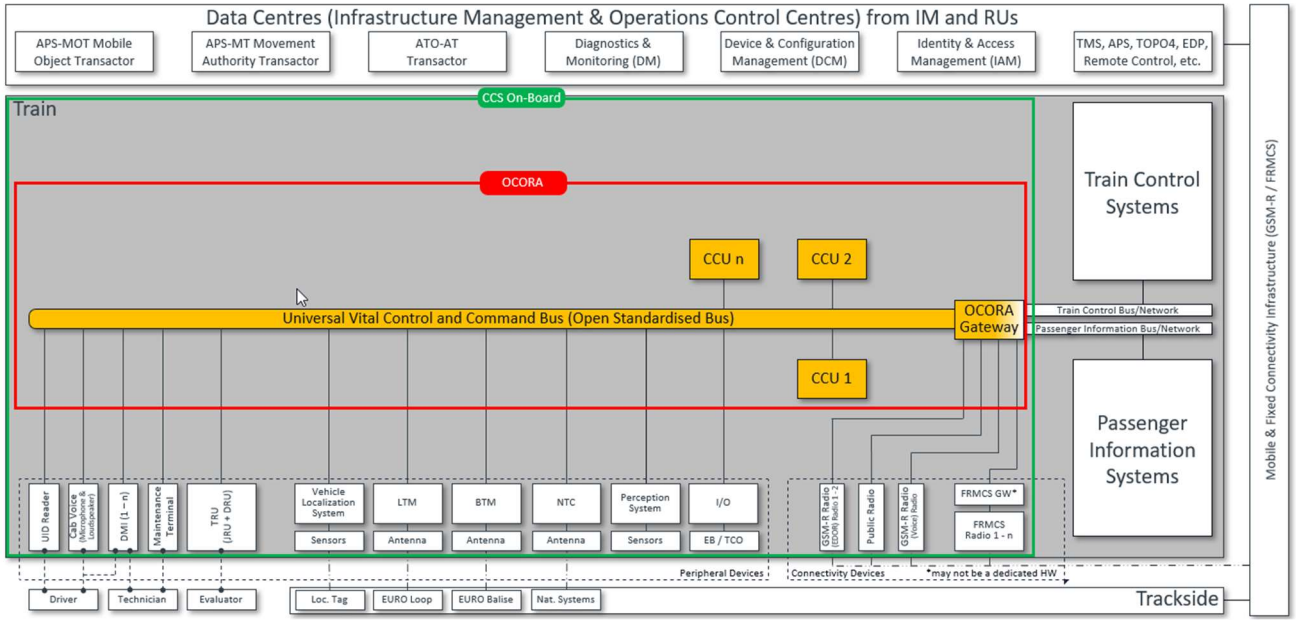

Figure 1 CCS onboard application platform reference architecture

A detailed description of the architecture is presented in OCORA-40-001-Beta – System Architecture [4].

2.4 Releases of this document and the security requirements

This version of the document serves as an overview and introduction of the cyber-security workstream for the OCORA Beta release. With the gamma release of OCORA a revised document and updated set of requirements will be published by the end of 2020.
The final document and set of security requirements will be available with the OCORA release 1.0.

3 Today's situation of security in railway

The primary goal of security in connection with systems or applications relevant for safety critical and availability critical operations must be to ensure that security incidents do not result in safety and operational or service incidents and that a minimal risk regarding safety and service is guaranteed.

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

For the most recent projects and projects in conception, cybersecurity is now more considered, and some enhancement is in progress, accomplished by creation and applying of international standards like the prTS 50701 [8] and the IEC 62443 3-3 [9].

3.1 Situation of security for railway operation

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

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

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

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

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

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

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

Railway is usually one of the biggest businesses in a country and has public access. Due to the size, passenger volume and high financial flow, a rail operator is an attractive target for attacks and needs to be secured.

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

3.2 Situation of security for rolling stock

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

In one of the attacks detected during the Honeytrain[1] project it was possible to activate the front lights of one simulated train. A command line was started, two PINGs were executed, and the execution program opened. It was found that the security configuration of industrial components was read out via a central tool, and the settings were exported. This points out that trains can also serve as a target for cyberattacks.

3.2.1 Modern trains

Cybersecurity considerations also apply to rolling stock. A modern train is effectively a mobile data center, communicating with the lineside equipment, the depot, the operational control center, traincrew, and the passengers. These information flows offer the hacker several potential entry points, all of which need to be carefully managed to mitigate the security threat.

3.2.2 Interoperability of trains

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

3.2.3 Physical security of trains

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

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

4 Strategy and approach

Chapter 3 has shown how important security solutions are for railway operators, therefore OCORA is required to consider security aspects of CCS on-board solutions as well. As mentioned in the Introduction to OCORA document [2] (cyber-) security is one of the main design goals (modularity, interoperability, replaceability, modifiability, adaptability, security and usability) for the OCORA reference architecture.

In European cooperation security experts from DB, NS, SBB, SNCF will develop a set of well-defined security requirements as an addition to the OCORA release 1.0 requirement catalogue. This will be achieved by creating and using a requirement defining process, workshops to define new security requirements and revisions of already existing ones.

4.1 Safety and security

Security is a base for providing safety. Assured integrity of communication and systems directly influences safety decisions. Nevertheless, for handling the two differing topics efficiently safety and security needs to be layered. For approval reasons it is necessary to separate the security solutions as far as possible from safety aspects so that security updates do not require a new safety certification. The “security as a shell” principle is to be the basis to achieve these design targets. A general separation is needed between security solutions that need a recertification and others that do not need it if changes (updates, upgrades) occur. With this separation only affected solutions must be recertified.

4.2 RAM and security

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

4.3 Normative background

The most important standards available for realizing security and safety related railway projects are EN 50126-1 [7], prTS 50701 [8] and IEC 62443 [9].

Figure 2 gives an overview and shows the partly overlapping in their aspects.

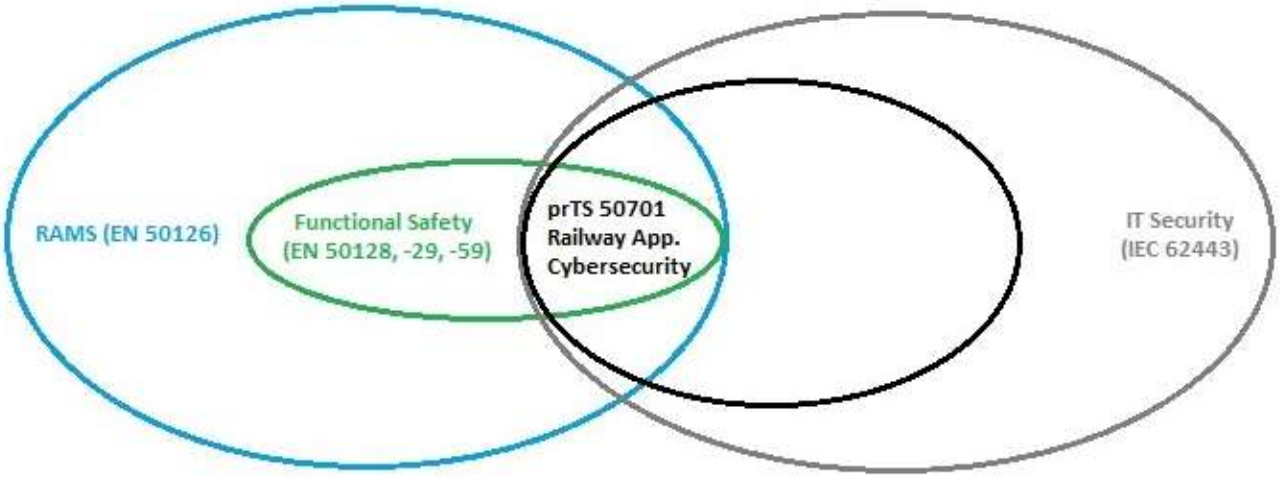

Figure 2 Railway standards

The standard prTS 50701 [8] combines the approaches from the CENELEC standard with the ones from the already established security standard IEC 62443 [9] (see Figure 3).

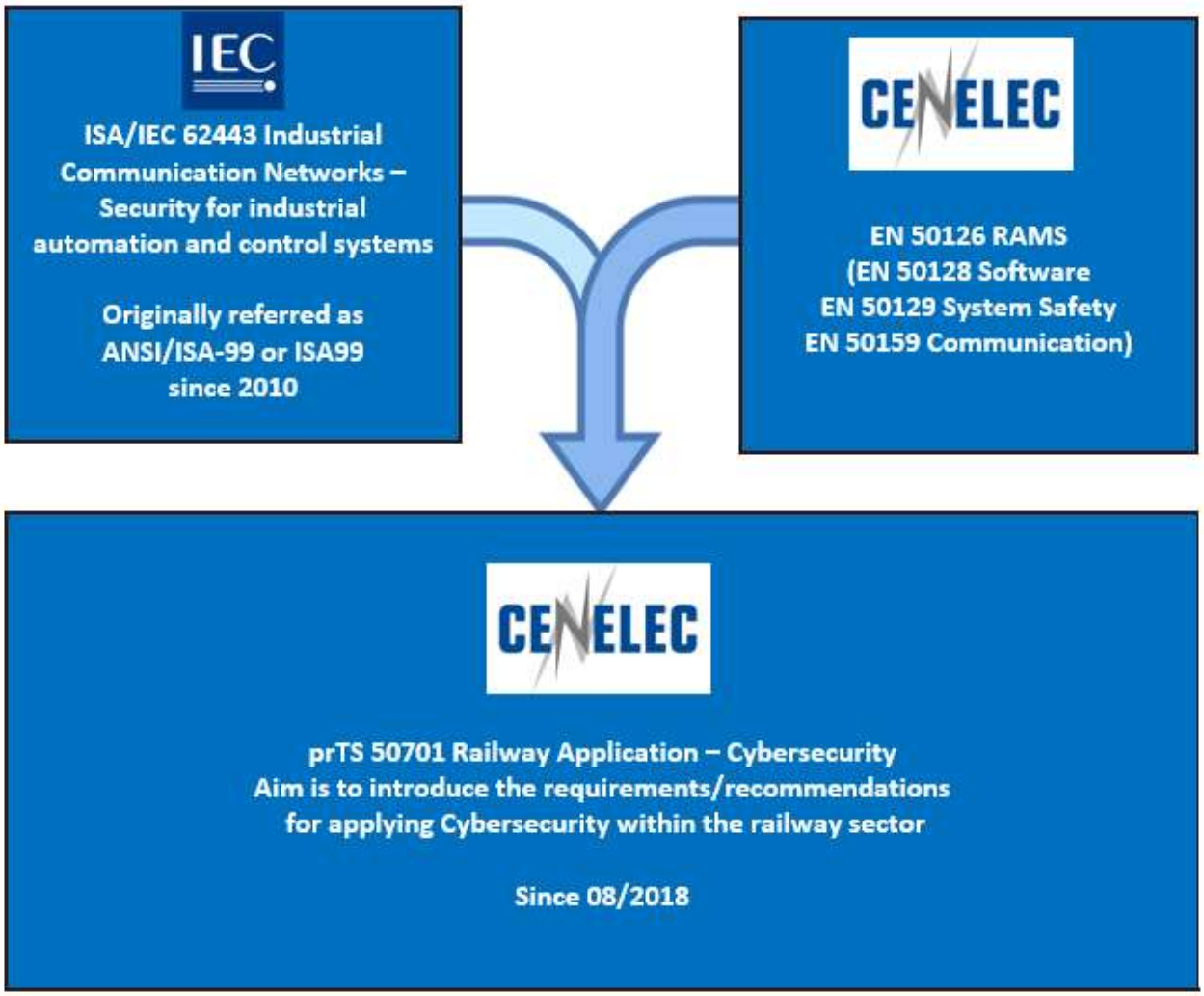

Figure 3 Development of prTS 50701

The base of prTS 50701 [8] is the V-Cycle (see Figure 4) from the CENELEC standard EN 50126-1 [7].

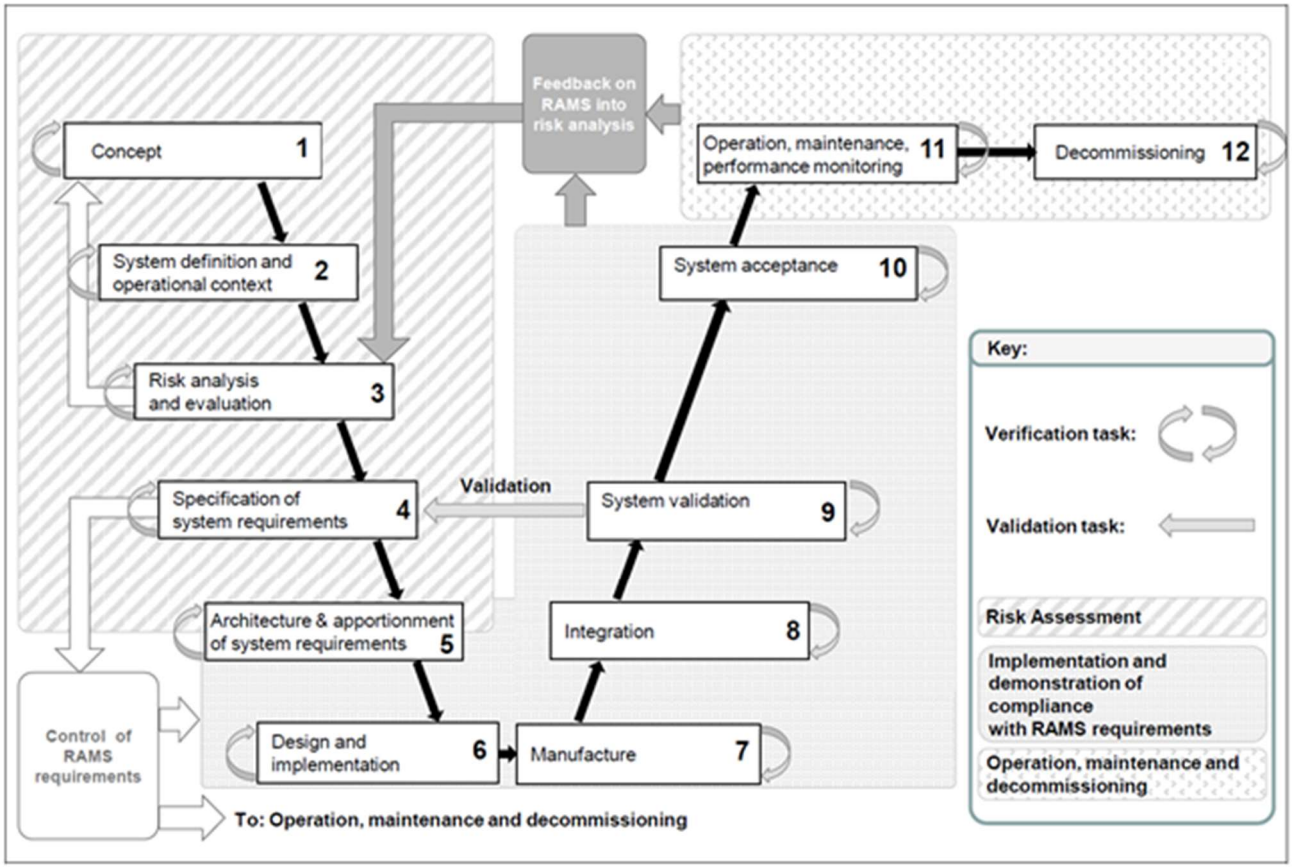

Figure 4 V-Cycle from EN 50126

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

Advantages of V-model:

- Simple and easy to use
- Testing activities like planning, test designing happens well before coding. This saves a lot of time
- Proactive defect tracking (defects are found at early stage)

Disadvantages of V-model:

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

The application of prTS 50701 [8] should be mandatory if security solutions are developed for safety related functions/systems. At the time of writing only a draft version of this standard is available, but the standard has already grown and evolved, and the final version should be available by the end of the year (2020).

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

Based on a threat analysis, structural analysis that follows the architecture, followed by a risk analysis shall define the relevant security level (SL) and TIER level (see Table 1 and Table 2).

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

Table 1 Security levels

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

Table 2 Tiers

The prTS 50701 [8] standard describes how this is to be used in the railway environment. It is relevant for the entire life cycle for development and documentation.

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

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

4.4 Security workstream

The focus of the OCORA security workstream will mainly be on the following points:

- Creation of security requirements as an addition for the OCORA requirement catalog
- Integration of (cyber-) security thoughts like zoning, principles and levels for the OCORA architecture

The workstream will also include opinions and results from other work groups. The following list provides a preliminary view of interfaces and tasks which are necessary for the OCORA security workstream:

- Compatibility with European NIS Directive and RCA reference architecture (EULYNX)
- Compatibility with TOBA project /FRMCS initiatives
- Integrate the results of the Shift2Rail program X2rail1 and X2rail2
- Contribution of ER-ISAC
- Possible participation in the X2rail4 program
- Definition of the responsibilities (integration testing and documentation)
- Clarification of independence from ATO standard (IRS 90940)
- Define which of the features must be tested and where (testbeds from smartrail 4.0, DB Netz, SBB Cyberlab)
- Ensure that the outcomes are short (e.g. through pointing to existing standards and security/maturity levels where possible).
- Security risk analysis process
- Definition and usage of a requirement process

The OCORA standardized architecture will define a centralized security component and services to all hosted applications into OCORA scope (with standardized interfaces). This standardized and centralized component may provide authenticate function for human and devices, log centralization, segregation with outside of OCORA scope.

5 Security requirements

The security requirements mentioned in Table 3 arise from the current perspective. The requirements will be completed with detailed security measures, defined through a risk based approach and a risk analysis to be performed in the second half-year of 2020.

The status of a requirement can be in review, approved or cancelled. After the approval of a requirement it will be transferred to the OCORA list of requirements [5].

Nr.	Security requirement	Status
1	Security level according shall be derived from IEC 62443 [9] after threat, architectural and risk analysis..	Approved
2	Maturity level must be derived from NIST CSF Tier 4 [10] after threat, architectural and risk analysis	Approved
3	Functions must be available for the following areas «identify, protect, detect, respond, recover» (corresponds to NIST CSF [10]).	Approved
4	The development and documentation of security solutions for the protection of safety and operational relevant systems shallbe according to prTS 50701 [8].	Approved
5	An STPAsec («System Theoretic Process Analysis for Security») must be carried out. An additional static design analysis should also be done.	Approved
6	The entire supply chain must be included in the security considerations.	Approved
7	The IT systems in the vehicle must be physically secured according to the state of the art (at least a Passepartout key). Also considering the circumstance that the vehicle is unlocked (depending on operations).	Approved
8	Separation of the security solutions as far as possible from safety aspects so that security updates do not require a new safety certification (security as a shell).	Approved

Table 3 Security requirements