OCORA

Open CCS On-board Reference Architecture

(Cyber-) Security Overview

Gamma Release

Document ID : OCORA-40-009-Gamma

Version : 1.00

Date: 04.12.2020

Status: Final

Revision history

Version	Change Description	Name (Initials)	Date of change
0.01	Draft for formal review	Roger Metz	2020-11-02
0.02	Security Cluster 1st review integration	Roger Metz	2020-11-12
1.00	OCORA formal review comments integration	Roger Metz	2020-12-04

Table of contents

Table of tables

Table of figures

References

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

The following references are used in this document:

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

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

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

[4] OCORA-30-006-Gamma – High Level Methodology

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

[6] OCORA-40-010-Gamma – (Cyber-) Security Strategy

[7] EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline

[8] OCORA-90-002-Gamma – Glossary

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

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

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

[12] prTS 50701 - Railway application - Cybersecurity

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

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

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

1 Management Summary

The advancing communication of components used in railway operations results in increased interfaces and points of contact between systems that are required for a state-of-the-art railway operation. Currently, there are no adequate and commonly used security solutions in place to protect against unauthorized access nor to completely prevent unauthorized interventions and attacks. This results in a steadily growing vulnerability to internal and external attacks on safety-relevant systems of a railway operator.

Therefore, OCORA is required to consider security aspects of CCS on-board solutions as well. Within a new European cooperation, security experts from DB, NS, SBB and SNCF are developing harmonized security processes, strategies and concepts.

The two main objectives of the OCORA security workstream for the Gamma Release was the creation of an adequate security engineering process. and that (cyber-) security thoughts get integrated in the OCORA architecture (e.g. zoning, principles, and levels).

The workstream also includes collaborations, opinions and results from other security work groups.

With the OCORA release 1.0 the final documentation will be available in 2021.

2 Introduction

2.1 Document Context and Purpose

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

Subsequent releases of this document (Delta, 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 treated on an international level
- an approach for a security risk management and how to define the security requirements
- a set of high-level on-board CCS security requirements

2.2 Why should I read this Document?

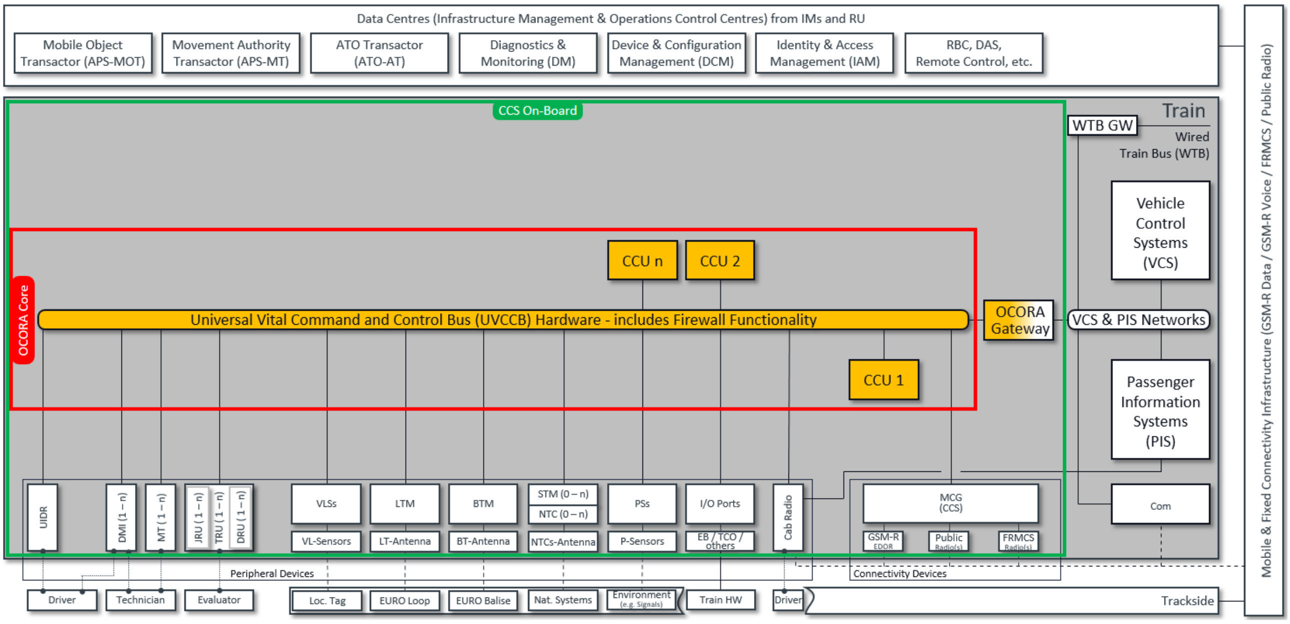
This document addresses experts in the railway security domain and any other person, interested in security engineering processes.

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

Prior to reading this document, it is recommended to read the Release Notes [1], the Introduction to OCORA [2] and the Problem Statements [3]. The reader should also be aware of the Glossary [8].

2.3 System under Consideration

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



Data Centres (Infrastructure Management & Operations Control Centres) from IMs and RU
Mobile Object Transactor (APS-MOT)
Movement Authority Transactor (APS-MT)
ATO Transactor (ATO-AT)
Diagnostics & Monitoring (DM)
Device & Configuration Management (DCM)
Identity & Access Management (IAM)
RBC, DAS, Remote Control, etc.
CCS On-Board
Train
WTB GW
Wired Train Bus (WTB)
Vehicle Control Systems (VCS)
OCORA Core
CCU n
CCU 2
Universal Vital Command and Control Bus (UVCCB) Hardware - includes Firewall Functionality
OCORA Gateway
VCS & PIS Networks
CCU 1
Passenger Information Systems (PIS)
UIDR
DMI (1 – n)
MT (1 – n)
JRU (1 – n)
TRU (1 – n)
DRU (1 – n)
VLSs
VL-Sensors
LTM
LT-Antenna
BTM
BT-Antenna
STM (0 – n)
NTC (0 – n)
NTCs-Antenna
PSs
P-Sensors
I/O Ports
EB / TCO / others
Cab Radio
MCG (CCS)
GSM-R EDOR
Public Radio(s)
FRMCS Radio(s)
Com
Peripheral Devices
Connectivity Devices
Driver
Technician
Evaluator
Loc. Tag
EURO Loop
EURO Balise
Nat. Systems
Environment (e.g. Signals)
Train HW
Driver
Trackside
Mobile & Fixed Connectivity Infrastructure (GSM-R Data / GSM-R Voice / FRMCS / Public Radio)

Figure 1 CCS onboard application platform reference architecture

A detailed description of the architecture is presented in OCORA-40-001-Gamma – System Architecture [5].

2.4 Releases of this Document

The first version of this document served as an overview and introduction of the (cyber-) security workstream for the OCORA Beta release.

This is the second version, and in addition to the overview/introduction, it acts now as a master document for the following security related documents created within the security workstream for the OCORA Gamma release:

- OCORA-40-009-Gamma – (Cyber-) Security Strategy [6]
- OCORA 40-011-Gamma – (Cyber-) Security Guideline [7]

It also has a set of high level (cyber-) security related non-functional requirement for the OCORA Gamma release.

The final documentation will be available with the OCORA Release 1.0 in 2021.

2.5 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, operational nor service incidents and that a minimized risk regarding safety and service is guaranteed.

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

For the most recent projects and projects in conception, cybersecurity is now more considered, and some enhancement is in progress, accomplished by creating and applying of international standards like the prTS 50701 [12] and the IEC 62443 [13] and with the related standardization initiatives like RCA (Reference CCS Architecture) and EULYNX.

2.5.1 Situation of Security for Railway Operation

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

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

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

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

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

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

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

[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

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

2.5.2 Situation of Security for Rolling Stock

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

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 via a central tool, and the settings were exported. This points out that trains can also serve as a target for cyberattacks.

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

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

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

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

[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

3 Security Workstream

OCORA's standardized architecture defines a centralized security component, which should host services with standardized interfaces to all applications into OCORA scope.

This standardized and centralized component provides authentication functions for humans and devices, centralized logging and segregation from the outside world. A segregation between applications or groups of applications hosted into OCORA scope and between applications hosted into OCORA with transversal services that uses the OCORA network (like log concentrator, security gateway, train-to-ground interface and maintenance port access) should be mandatory.

Chapter 2.5 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) this includes:

- Creation of a security process (including security risk management) to achieve a well-founded security concept and requirements (see EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7]).
- Ensure that the security requirements are short formulated (e.g. through pointing to existing standards and security/maturity levels where possible).

For information about the organizational structure, scope, main targets and deliveries from OCORA please refer to the document OCORA-30-001-Gamma – Introduction to OCORA [2].

3.1 Main Topics

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

- Creation of a security process with risk management
- Integration of (cyber-) security thoughts like zoning and security principles for the OCORA architecture
- Security Strategy
- Security Concept
- Security Requirements

3.2 Security Interfaces

3.2.1 Safety and Security

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

3.2.2 RAM and Security

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

3.2.3 Other Interfaces

The security workstream also includes collaboration with other work groups and uses results from other work groups.

Topics interfacing with other work groups:

- Compatibility with European NIS Directive and RCA (reference ccs architecture) and EULYNX (Risk Management approach mapping)
- 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

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

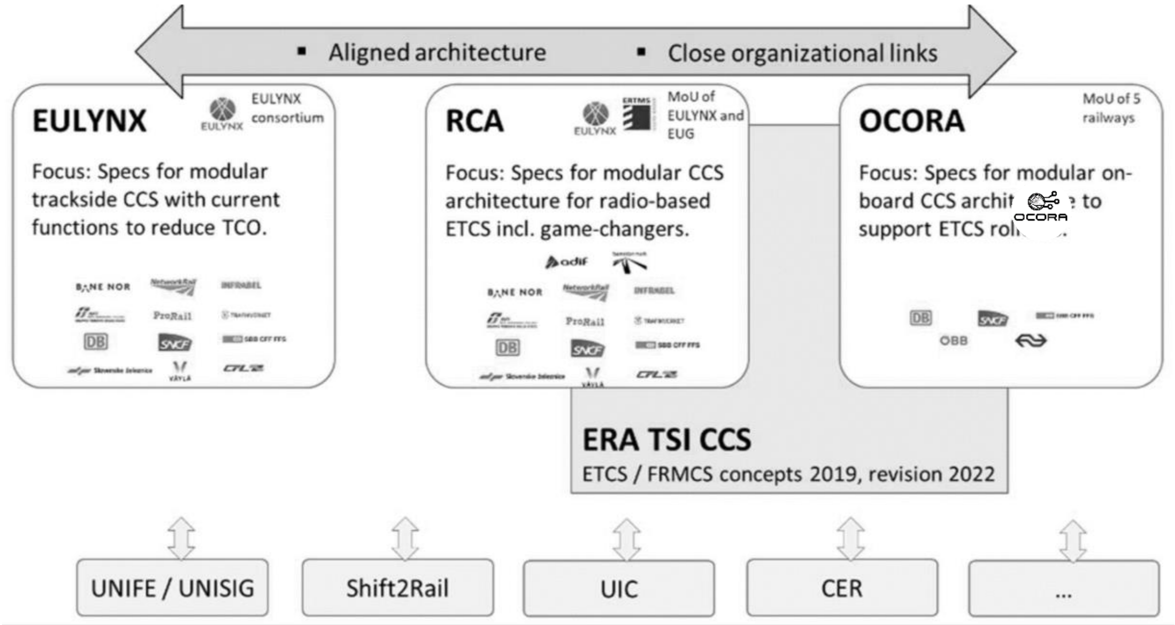

▪ Aligned architecture
▪ Close organizational links
EULYNX
EULYNX consortium
Focus: Specs for modular trackside CCS with current functions to reduce TCO.
RCA
MoU of EULYNX and EUG
Focus: Specs for modular CCS architecture for radio-based ETCS incl. game-changers.
OCORA
MoU of 5 railways
Focus: Specs for modular on-board CCS archit... to support ETCS rol...
ERA TSI CCS
ETCS / FRMCS concepts 2019, revision 2022
UNIFE / UNISIG
Shift2Rail
UIC
CER
...

Figure 2 Relations of EULYNX, RCA and OCORA[1]

3.3 Security Process

The approach is harmonised and consolidated with the EULYNX/RCA work groups. Please refer to the document EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7] for a detailed description of the security process. It covers the following aspects:

- V-cycle/model mapping
- Process evaluation
- Process (Tools)
- Guideline/Walkthrough

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

A detailed description of the OCORA-V-cycle can be found in OCORA-30-006-Gamma – High Level Methodology [4]. It provides information about the following aspects and how they are defined:

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

3.4 Security Strategy

This Document gives a deep look at security strategies. Please refer to the document OCORA-40-010-Gamma – (Cyber-) Security Strategy [6].

3.5 Security Guideline

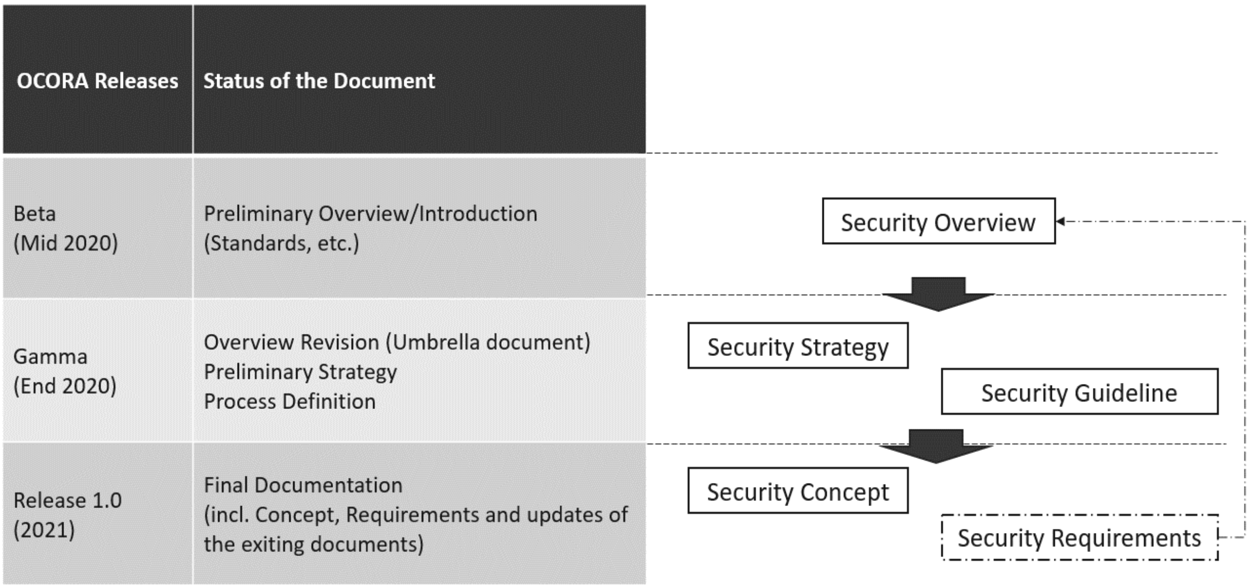
This Document gives a deep look and walkthrough of the security process. Please refer to the document EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7]. This Document will be available after the formal RCA, EULYNX & OCORA approval processes.

3.6 Security Concept

The OCORA security concept will be available after all security tasks (defined in the EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7]) are completely carried out. It will be released with the OCORA Release 1.0 in 2021.

3.7 Documentation Overview

Figure 3 shows the chronological order and dependencies of the OCORA security document landscape. The Security Requirements will be added to the list in chapter 5.



OCORA Releases	Status of the Document
Beta (Mid 2020)	Preliminary Overview/Introduction (Standards, etc.)
Gamma (End 2020)	Overview Revision (Umbrella document) Preliminary Strategy Process Definition
Release 1.0 (2021)	Final Documentation (incl. Concept, Requirements and updates of the exiting documents)

Figure 3 OCORA Security Documentation

4 Normative Background

The following chapters show the fundamental basis for the security activities which must be followed during the development of security solutions.

4.1 Railway Standards

The most important standards currently available for realizing security and safety related railway projects are EN 50126-1 [9], EN 50129 [10], EN 50159 [11], and IEC 62443 [13]. Figure 4 gives an overview and shows the partly overlapping in their aspects.

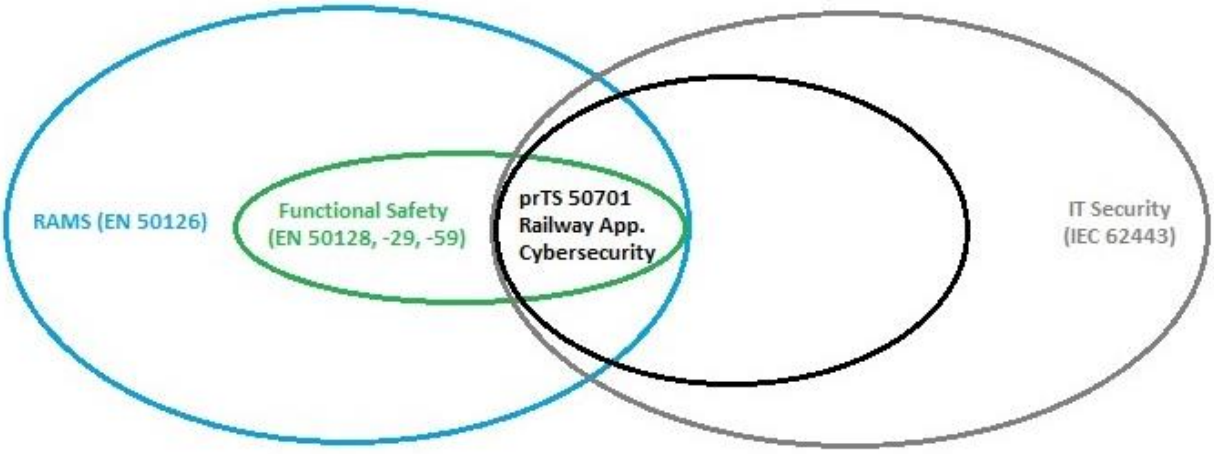


Figure 4 Railway standards

The standard prTS 50701 [12] combines the approaches from the CENELEC standard with the ones from the already established security standard IEC 62443 [13] (see Figure 5).

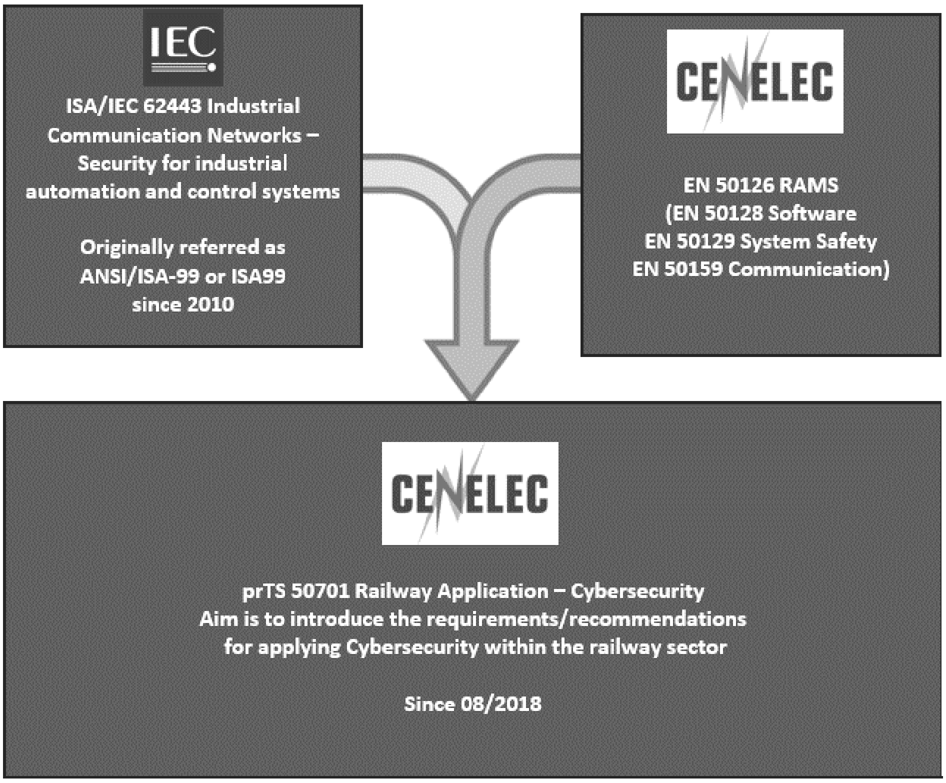

IEC
ISA/IEC 62443 Industrial Communication Networks – Security for industrial automation and control systems
Originally referred as ANSI/ISA-99 or ISA99 since 2010
CENELEC
EN 50126 RAMS
(EN 50128 Software
EN 50129 System Safety
EN 50159 Communication)
CENELEC
prTS 50701 Railway Application – Cybersecurity
Aim is to introduce the requirements/recommendations for applying Cybersecurity within the railway sector
Since 08/2018

Figure 5 Development of prTS 50701

The base of prTS 50701 [12] is the V-Cycle (see Figure 6) from the CENELEC standard EN 50126-1 [9].

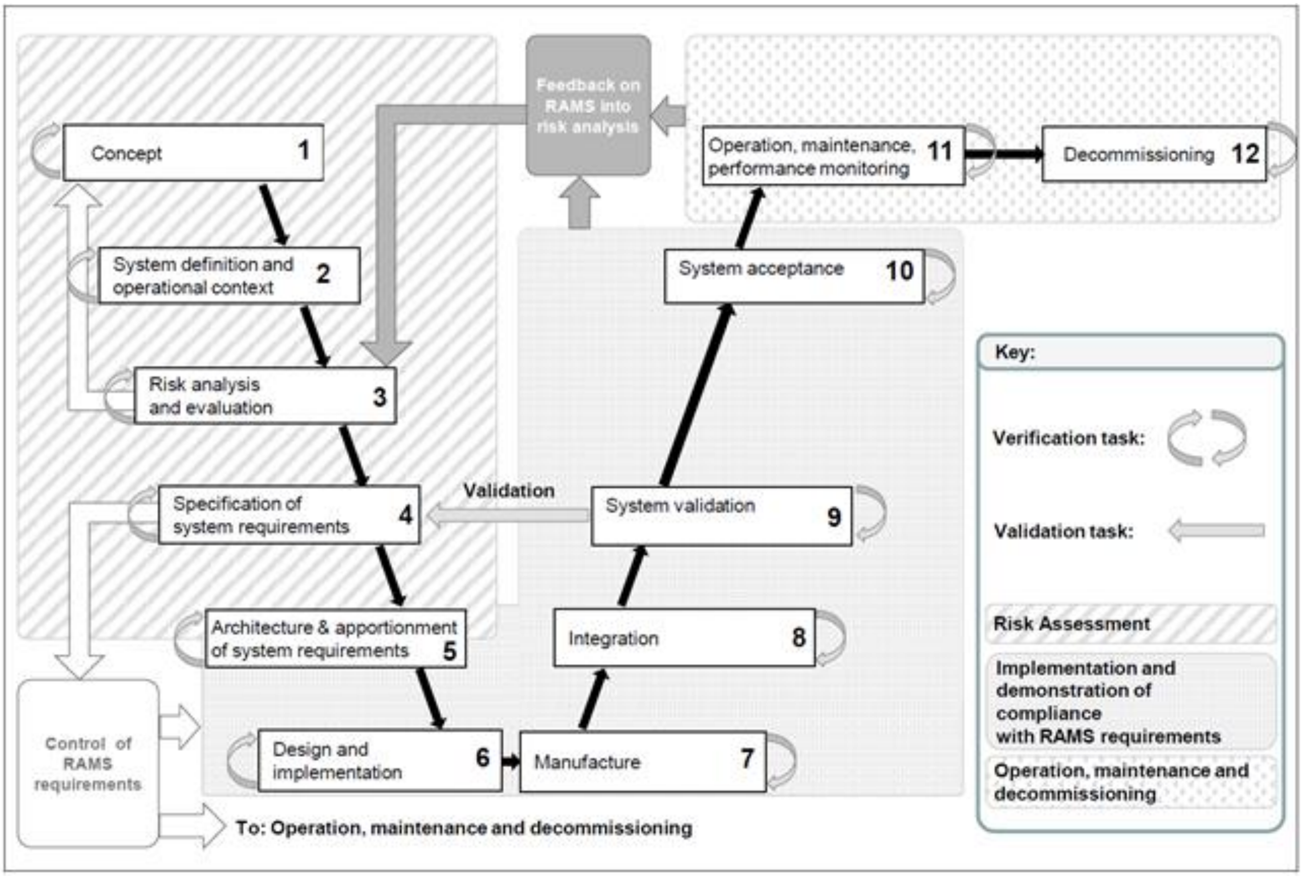

Feedback on RAMS into risk analysis
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
Control of RAMS requirements
To: Operation, maintenance and decommissioning
Key:
Verification task:
Validation task:
Risk Assessment
Implementation and demonstration of compliance with RAMS requirements
Operation, maintenance and decommissioning

Figure 6 V-Cycle EN 50126

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

Advantages of V-model:

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

Disadvantages of V-model:

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

The prTS 50701 standard defines the base principles how security (prTS 50701 [12]) and safety (EN 50126 [9]) must be handled. The statements of impact of security to safety lists the following:

- Principle 1:
  Safety and security are different and should be treated as such.
- Principle 2:
  The security environment shall protect essential functions, incl. safety.
- Principle 3:
  Threat & risk analysis is the main interface with safety analysis.

- Principle 4:
  Separate security and safety as far as possible but coordinate them effectively.
- Principle 5:
  Security shall be evaluated based on international standards, e.g. IEC 62443.
- Principle 6:
  It is impossible to evaluate the security risk probabilistically.
- Principle 7:
  Safety and security target measures shall not be coupled.

The following guidance can be considered according prTS 50701:

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

More details about safety synchronisation and cybersecurity assurance are presented in the EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7].

The application of prTS 50701 [12] 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 2021.

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

Based on a threat analysis, structural analysis that follows the architecture, followed by a risk analysis shall define the relevant Security Level (Table 1), TIER level (see Table 2) or Maturity Level (see Table 3). The NIST Cybersecurity Implementation Tiers are a scaled ranking system that describes the degree to which an organization exhibits the characteristics described in the NIST Cybersecurity Framework.

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

The application of the Security Levels is demonstrated in the document EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7].

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

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

Maturity Level	Name	Description
1	Initial	Product suppliers typically perform product development in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency across projects and repeatability of processes may not be possible.
2	Managed	At this level, the product supplier has the capability to manage the development of a product according to written policies (including objectives). The product supplier also has evidence to show that personnel who will perform the process have the expertise, are trained and/or follow written procedures to perform it. However, at this level, the organization does not have experience developing products to all the written policies. This would be the case when the organization has updated its procedures to conform to this document but has not yet put all the procedures into actual practice, yet. The development discipline reflected by maturity level 2 helps to ensure that development practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans. NOTE: At this level, the CMMI and IEC 6 2443-4-1 maturity models are fundamentally the same, with the exception that IEC 6 2443-4-1 recognizes that there may be a significant delay between defining/formalizing a process and executing (practicing) it. Therefore, the execution related aspects of the CMMI-DEV Level 2 are deferred to Level 3.
3	Defined (Practiced)	The performance of a level 3 product supplier can be shown to be repeatable across the supplier’s organization. The processes have been practiced, and evidence exists to demonstrate that this has occurred. NOTE: At this level, the CMMI and IEC 62443-4-1 maturity models are fundamentally the same, with the exception that the execution related aspects of the CMMI-DEV level 2 are included here. Therefore, a process at level 3 is a level 2 process that the supplier has practiced for at least one product.
4	Quantitatively Managed	At this level, IEC62443-4-1 combines CMMI-DEV levels 4 and 5. Using suitable process metrics, product suppliers control the effectiveness and performance of the product and demonstrate continuous improvement in these areas.
5	Optimizing	See ML4

Table 3 Maturity Level

The prTS 50701 [12] standard describes how this is to be used in the railway environment. It is relevant for the entire life cycle for development and documentation.

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

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

4.2 IT Security Risk Management and Process

Risk management is an ongoing iterative and continuous process usually distributed over several CENELEC phases. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerabilities emerge every day. The choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

Definition of risk management:

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

Generally speaking, risk is the product of likelihood times impact (Risk = Likelihood * Impact)

The IT risk management has mainly three aims:

- The protection of IT systems that store, process and transfer company data to the level that is necessary to operate them legally and at the security level adapted for the company.
- Providing the management with the necessary information and transparency to correctly assess risks and to make good decisions about investing in security measures.
- Providing the management with documentation that helps them understand the effectiveness of security measures and their impact on risks.

There are four main ways how to handle recognized risks:

- Avoid (stop the development of the product or outsourcing)
- Accept (take the risk and do nothing about risk reduction)
- Reduce (define measures and reduce the risk)
- Transfer (outsourcing with contractual risk assumption, insurance)

The usability, appearance/design and level of detail vary from the different processes provided by the main security standards out there. For example, the NIST risk flowchart has changed over time and was simplified. The version from 2002 has more details in terms of process steps an interaction.

A detailed evaluation of the most common processes from standards is presented in the EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7], which leads to the security process introduced in the guideline and also has an example walkthrough to make the process more tangible.

5 Security Requirements

The security requirements mentioned in Table 4 arise from the current perspective and have been defined in workshops.

The requirements for the final release of OCORA will be completed with detailed security measures, defined through a risk-based approach and risk analysis. Described in EULYNX-RCA-OCORA-40-011-Gamma – (Cyber-) Security Guideline [7].

The status of a requirement can be in review, approved or cancelled.

Nr.	Security requirement	Status
1	Security level according to IEC 62443 [13] shall be derived after threat, architectural and risk analysis for all security solutions.	Approved
2	Maturity level according to to NIST CSF [14] shall be derived after threat, architectural and risk analysis for all security solutions.	Approved
3	Functions must be available for the following areas «identify, protect, detect, respond, recover» (corresponds to NIST CSF [14]).	Approved
4	The development and documentation of security solutions for the protection of safety and operational relevant systems shall be according to prTS 50701 [12].	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 4 Security requirements

END OF DOCUMENT