OCORA

Open CCS On-board Reference Architecture

Project Security Management Plan (PSMP)

Document ID: OCORA-TWS06-010

Version: 3.00

Date: 08.06.2022

Management Summary

The document is a generic description of a Project Security Management Plan (PSMP) that can be used as a template that covers the phases 0 to 5 specified in Table 1 of the TS 50701 [11]. The document is based on the structure according to Annex G.2 of the TS 50701 [11]. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

To ensure the necessary stability and viability of safety-related documentation and approval, it is advisable to separate cybersecurity and safety issues as far as possible and coordinate them adequately in order to decouple the different lifecycles and the approval processes. Otherwise, each change affecting the security of the system may trigger a new safety approval. Therefore, cybersecurity measures affecting the safety of the SuC shall be changed until they no longer impact the safety of the SuC. This is necessary to prevent the CCS or any of its subsystems from losing its safety integrity, and thus its approval, due to a new cyber threat or its defence against it.

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Delta Release	RME	30.06.2021
2.00	Official version for OCORA Release R1	RME	30.11.2021
2.01	Initial draft of general update	ZE	27.04.2022
2.02	Review of document	SSt, MSc, PhN	04.05.2022
2.03	Clean version without tracked changes, reference list shortened, references updated	SSt	23.05.2022
2.04	TWS review comments incorporated	SSt	02.06.2022
3.00	Official version for OCORA Release R2	SSt	08.06.2022

Table of contents

Table of figures

Table of tables

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

[8] OCORA-TWS06-30 – (Cyber-) Security Concept

[9] EN 50126-1:2017-10, "Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process", European Committee for Electrotechnical Standardization (CENELEC), October 2017.

[10] EN 50126-2:2017-10, "Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety", European Committee for Electrotechnical Standardization (CENELEC), October 2017.

[11] TS 50701: 2022, "Railway applications – Cybersecurity", European Committee for Electrotechnical Standardization (CENELEC), 7. January 2022.

[12] IEC/TS 62443-1-1: 2009-07, "Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models ", International Electrotechnical Commission (IEC), Edition 1.0, July 2009.

[13] 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.

[14] IEC/TR 62443-2-3: 2015-06, "Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment", International Electrotechnical Commission (IEC), Edition 1.0, June 2015.

[15] 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.

[16] IEC/TR 62443-3-1: 2009-07, "Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems", International Electrotechnical Commission (IEC), Edition 1.0, July 2009.

[17] 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.

[18] IEC 62443-3-3: 2013-08, "Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels", International Electrotechnical Commission (IEC), Edition 1.0, August 2013.

[19] 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.

[20] IEC 62443-4-2: 2019-02, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components", International Electrotechnical Commission (IEC), Edition

1.0, February 2019.

[21] ISO 27001: 2013-10, “Information Technology – Security Techniques – Information Security Management Systems – Requirements”, International Organization for Standardization (ISO), October 2013.

[22] ISO 9001: 2015-09, “Quality Management Systems”, International Organization for Standardization (ISO), 5th Edition, 15.09.2015.

1 Introduction

1.1 Purpose of the document

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader 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.

The project security management plan (PSMP) defines the cybersecurity related tasks carried out throughout the whole lifecycle of the system. The purpose of the document is:

a) to plan the management of the cybersecurity activities,

b) to define the cybersecurity context,

c) to plan the cybersecurity risk management,

d) to describe the design of the cybersecurity,

e) to define the secure development lifecycle,

f) to specify the acceptance of the cybersecurity assurance,

g) to manage the vulnerabilities and the cybersecurity issues, and

h) to manage the third parties risk management

The document is based on the structure according to Annex G.2 of the TS 50701 [11].

At this point in time, the PSMP focuses on the phases 0 to 5.

1.2 Applicability of the document

The document is a generic description of PSMP that can be used as a template if the approval process of a formally project is started. So far, the content up to chapter 3.3 is elaborated Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

This “Project Security Management Plan” (PSMP) applies to Phase 0 through 5 specified in Table 1 of the TS 50701 [11], i.e.

Phase 0: Prerequisites,

Phase 1: Concept,

Phase 2: System definition and operational context,

Phase 3: Risk analysis and evaluation, and

Phase 4: Specification of system requirements.

Phase 5: System architecture

The extension of this PSMP to include the phases 6 through 12 will take place in subsequent releases of the document.

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 Cybersecurity Activities Management

2.1 Overview

The Cybersecurity Activities Management chapter introduces:

- the organisational structures
- the roles responsibilities and competences
- the cybersecurity skills and training of the cybersecurity team
- the interfaces with the stakeholders
- the key milestones
- the communication and reporting

2.2 Project Organization Chart

2.2.1 Overview

The objective of the project organization is to ensure that all personnel who have responsibilities for the cybersecurity are organised, empowered and capable of fulfilling their responsibilities.

Independence between roles is required to ensure that people in different roles do not suffer from the same misconceptions or making the same mistakes. This form of independence can be achieved by employing different people in different roles but does not usually require the roles to be located in different parts of the organisation or in different companies.

It is also important that people in roles which involve making judgements about the acceptability of the cybersecurity product or process shall not be influenced by pressure from their peers or supervisors, or by considerations of commercial gain.

The organisational structures are based on the safety standard EN 50126-2 [10].

2.2.2 Objectives

- As a minimum, the supplier shall implement the relevant parts of EN ISO 9001 [22] and ISO 27001 [21] dealing with the organisation and management of the personnel and responsibilities.
- Responsibilities shall be compliant with the requirements defined in chapter 0 entitled “Annex A: Key Cybersecurity Roles and Responsibilities”.
- The personnel assigned to the roles involved in the development or maintenance of the cybersecurity shall be named and recorded.
- If an Assessor is required, the Assessor shall be appointed by the supplier, the customer or the Cybersecurity Authority.
- The Assessor shall be independent from the supplier or, at the discretion of the Cybersecurity Authority, be part of the supplier’s organisation or of the customer’s organisation.
- The Assessor shall be independent from the project.
- The Assessor shall be given authority to perform the assessment of the cybersecurity.
- The Validator shall give agreement/disagreement for the cybersecurity release.
- Throughout the Cybersecurity Lifecycle, the assignment of roles to persons shall be in accordance with 2.2.3 to 2.2.7, to the extent required by cybersecurity SL.
- The System / security Administrator (SAD) shall not report to the Project Manager (PM) for any Security Level (SL).

- The System / security Administrator (SAD) can be of the same organisation for any Security Level (SL).

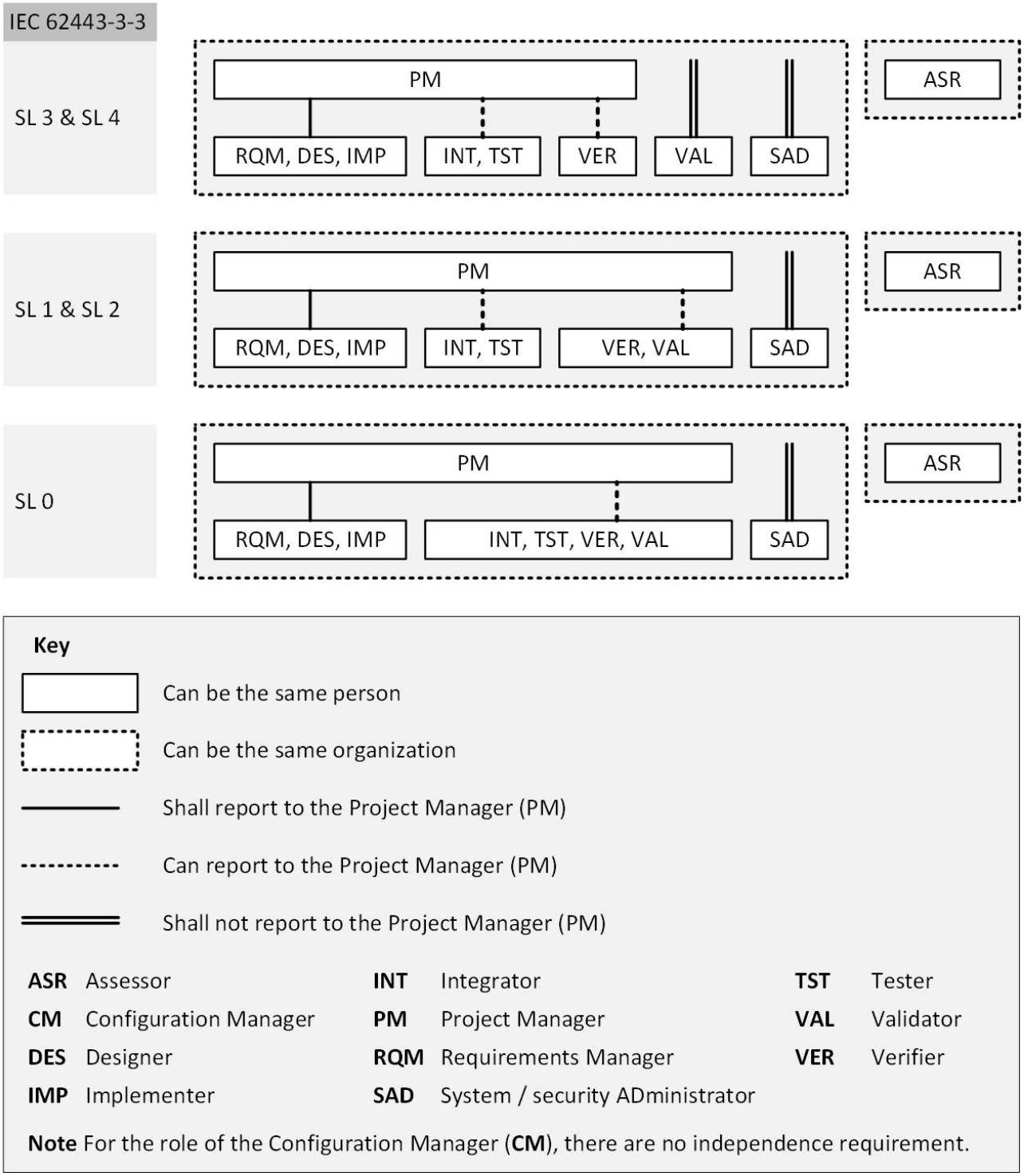

Figure 1: Project organisation chart

2.2.3 The preferred organisational structure for SL 3 and SL 4

a) Requirements Manager, Designer and Implementer for a cybersecurity-related component can be the same person.

b) Requirements Manager, Designer and Implementer for a cybersecurity-related component shall report to the Project Manager.

c) Integrator and Tester for a cybersecurity-related component can be the same person.

d) Integrator and Tester for a cybersecurity-related component can report to the Project Manager or to the Validator.

e) Verifier can report to the Project Manager or to the Validator.

f) Validator shall not report to the Project Manager i.e. the Project Manager shall have no influence on the validator's decisions but the validator informs the Project Manager about his decisions.

g) A person who is Requirements Manager, Designer or Implementer for a cybersecurity-related component shall neither be Tester nor Integrator for the same cybersecurity-related component.

h) A person who is Integrator or Tester for a cybersecurity-related component shall neither be Requirements Manager, Designer nor Implementer for the same cybersecurity-related component.

i) A person who is Verifier shall neither be Requirements Manager, Designer, Implementer, Integrator, Tester nor Validator.

j) A person who is Validator shall neither be Requirements Manager, Designer, Implementer, Integrator, Tester nor Verifier.

k) A person who is Project Manager can additionally perform the roles of Requirements Manager, Designer, Implementer, Integrator, Tester or Verifier providing that the requirements for the independence between these additional roles are respected.

l) Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and Validator can belong to the same organization.

m) The assessor shall be independent and organisationally independent from the roles of Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and Validator.

However, the following options may apply:

n) A person who is Validator may also perform the role of Verifier, but still maintaining independence from the Project Manager. In this case the Verifier's output documents shall be reviewed by another competent person with the same level of independence as the Validator. This organisational option shall be subject to Assessor's approval.

o) A person who is Verifier may also perform the role of Integrator and Tester, in which case the role of Validator shall check the adequacy of the documented evidence from integration and testing with the specified verification objectives, hence maintaining two levels of checking within the project organisation.

2.2.4 The preferred organisational structure for SL 1 and SL 2

a) Requirements Manager, Designer and Implementer for a cybersecurity-related component can be the same person and shall report to the Project Manager.

b) Integrator and Tester for a cybersecurity-related component can be the same person.

c) Integrator and Tester for a cybersecurity-related component can report to the Project Manager or to the Validator.

d) Verifier and Validator can be the same person.

e) Verifier and Validator can report to the Project Manager.

f) A person who is Requirements Manager, Designer or Implementer for a cybersecurity-related component shall be neither Tester nor Integrator for the same cybersecurity-related component.

g) A person who is Integrator or Tester for a cybersecurity-related component shall neither be Requirements Manager, Designer nor Implementer for the same cybersecurity-related component.

h) A person who is Verifier or Validator shall neither be Requirements Manager, Designer, Implementer, Integrator nor Tester.

i) A person who is a Project Manager can additionally perform the roles of Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier or Validator provided that the requirements for the independence between these additional roles are respected.

j) Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and

Validator can belong to the same organization.

k) The assessor shall be independent and organisationally independent from the roles of Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and Validator.

However, the following options can apply:

l) A person who is Verifier may also perform the role of Integrator and Tester, in which case the role of Validator shall include reviewing the Verifier's output documents hence maintaining two levels of checking within the project organisation.

m) A person who is Validator may also perform the role of Verifier, Integrator and Tester. In this case the Verifier's output documents shall be reviewed by another competent person with the same level of independence as the Validator. This organisational option shall be subject to Assessor's approval.

2.2.5 The preferred organisational structure for SL 0

a) Requirements Manager, Designer and Implementer for a cybersecurity component can be the same person and shall be managed by the Project Manager.

b) Integrator, Tester, Verifier and Validator for a cybersecurity component can be the same person.

c) Integrator, Tester, Verifier and Validator can be managed by the Project Manager.

d) A person who is Requirements Manager, Designer or Implementer for a cybersecurity component shall be neither Tester nor Integrator for the same cybersecurity component.

e) A person who is Verifier or Validator shall neither be Requirements Manager, Designer, nor Implementer.

f) A person who is Project Manager can additionally perform the roles of Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier or Validator providing that the requirements for the independence between these additional roles are respected.

g) Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and Validator can belong to the same organization.

h) The assessor shall be independent and organisationally independent from the roles of Project Manager, Requirements Manager, Designer, Implementer, Integrator, Tester, Verifier and Validator.

However, the following alternatives can apply:

i) Requirements Manager, Designer, Implementer, Integrator and Tester can be the same person.

j) The Validator and Verifier can also be the same person.

k) A person who is Verifier or Validator shall neither be Requirements Manager, Designer, nor Implementer.

2.2.6 Accumulation of Roles

The roles Requirements Manager, Designer and Implementer for one component can perform the roles Tester and Integrator for a different component.

2.2.7 Roles to be Maintained throughout the Project

The roles of the Verifier and the Validator shall be defined at the project level and shall remain unchanged throughout the development project.

2.3 Roles and Responsibilities Related to Cybersecurity Activities

The roles introduced in section 2.2 are detailed regarding the associated

- responsibilities and
- key competences

in chapter 4 entitled “Annex A: Key Cybersecurity Roles and Responsibilities”.

2.4 Project Team Cybersecurity Skills and Training Needs

2.4.1 Project Team Cybersecurity Skills

2.4.1.1 Overview

Because cybersecurity of the CCS OB system involves several different sets of skills not often found in any one particular section or department of an organization, it is imperative that senior leadership formulate an approach to managing security with clear identification of accountability and responsibility that makes good use of skills and labor resources not typically found in any single person. The team should include people with the following roles:

- CCS person(s) who may be implementing and supporting the CCS OB devices.
- operations person(s) responsible for making the product and meeting customer orders.
- process safety management person(s) whose job it is to ensure that no health, safety and environmental incidents occur.
- IT person(s) who may be responsible for network design and operation, support of desktops and servers, and the like.
- security person(s) associated with physical and IT security at the site.
- additional resources who may be in the legal, human resources and customer support or order fulfilment roles.

The project team cybersecurity shall cover

1. general cybersecurity skills for all personnel and
2. role-based cybersecurity skills aimed at specific duties and responsibilities.

2.4.2 General Cybersecurity Skills

The general cybersecurity skills for all personnel shall aim at

- preventing the unauthorized disclosure of information;
- preventing the casual or coincidental circumvention of zone and conduit segmentation;
- ensuring that the control system operates reliably under normal and abnormal production conditions and prevents Denial-of-Service (DoS) situations;
- identifying and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access;
- restricting use of the CCS according to specified privileges to protect against circumvention; and
- protecting the integrity of the CCS against manipulation.

2.4.2.1 Role-Based Cybersecurity Skills

The role-based cybersecurity skills are listed for each role in chapter 4 entitled “Annex A: Key Cybersecurity Roles and Responsibilities“.

Additionally, the skills of the system/security administrator (SAD) shall include

- strong familiarity with the operating system and its networking components;
- good understanding of the application and its environmental prerequisites;
- awareness of how the patch should interact with the application and operating system and what the possible consequences of the upgrade may be; and

- monitoring capabilities of the operation of the CCS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried.

2.4.3 Training Needs

2.4.3.1 Training Requirements

Training programs should be in place for new hires, operations, maintenance, upgrades and succession planning. Training programs should be well documented, structured, and updated at regular intervals to incorporate changes in the operating environment.

All personnel should receive adequate technical training associated with the known threats and vulnerabilities of hardware, software and social engineering.

The staff training and security awareness is compiled in Table 1. The training shall be in two phases:

1. general training for all personnel and
2. role-based training aimed at specific duties and responsibilities.

Before beginning the development of the training program it is important to identify the scope and boundaries for the training and to identify and define the various roles within the organization.

Description	Requirements	Content of training
Develop a training program	The organisation shall design and implement a cyber security training program.	Training of one sort or another is an activity that spans almost the entire period during which a CSMS is developed and implemented. It begins after the scope of the effort is clarified and the team of stakeholders is identified. The objective of the training program is to provide all personnel with the information they need so that they will be aware of any possible threats to the system and their responsibilities for the safe and secure operation of the production facilities.
Provide procedure and facility training	**All personnel** (including employees, contract employees, third-party contractors) shall be trained initially and periodically thereafter in the correct security procedures and the correct use of information processing facilities including include legal responsibilities, business controls and individual security responsibilities. **Role-based training** should focus on the security risks and responsibilities associated with the specific role a person fills within the organization.	General and role-based staff training including security awareness programs shall provide all personnel (employees, contractors, and the like) with the information necessary to • identify, • review, • address and where appropriate, • remediate vulnerabilities and threats to the CCS OB system and to help ensure their own work practices include effective countermeasures.
Provide training for support personnel	All personnel that perform risk management, CCS OB engineering and system administration / maintenance and other tasks that impact the Cyber Security Management System (CSMS) should be trained on the security objectives and operations for these	General and role-based staff training including security awareness programs shall provide all personnel (employees, contractors, and the like) with the information necessary to • identify, • review, • address and where appropriate,

	tasks.	• remediate vulnerabilities and threats to the CCS OB system and to help ensure their own work practices include effective countermeasures.
Validate the training program	The training program shall be validated on an on-going bases to ensure that the personnel understand the “Security Program” (see Annex B in chapter 5) and that they are receiving the proper training.	It is important to validate those personnel are aware of their roles and responsibilities as part of the training program. Validation of security awareness provides two functions: 1. it helps identify how well the personnel understand the organization’s cyber “Security Program” (see Annex B in chapter 5) and 2. it helps to evaluate the effectiveness of the training program. Validation can come through several means including written testing on the content of the training, course evaluations, monitored job performance or documented changes in security behaviour. A method of validation should be agreed upon during the development of the training program and communicated to the personnel.
Revise the training program over time	The “Security Program” (see Annex B in chapter 5) shall be revised, as necessary, to account for new or changing threats and vulnerabilities.	Over time, the vulnerabilities, threats and associated security measures will change. These changes will necessitate changes to the content of the training program. The training program should be reviewed periodically (for example, annually) for its effectiveness, applicability, content and consistency with tools currently used and corporate practices and laws and revised as needed. Subscriptions to security alert services may help ensure up-to-date knowledge of recently identified vulnerabilities and exposures.
Maintain employee training records	Records of employee training and schedules for training updates shall be maintained and reviewed on a regular basis.	Records of employee training and schedules for training updates should be maintained and reviewed on a regular basis. Documenting training can assist the organization to ensure that all personnel have the required training for their particular roles and responsibilities. It can also help identify if additional training is needed and when periodic retraining is required.

Table 1: Staff training and security awareness

2.4.3.2 Baseline practices

The following seven actions are baseline practices:

a. Addressing the various roles associated with maintaining a secure systems environment within the cyber security training curriculums.

b. Having classroom courses or on-the-job training to address the requirements for each role.

c. Validating a user’s understanding via course evaluations and/or examinations.

d. Having subject matter experts for each course who can provide additional information and consulting.

e. Reviewing and validating the training curriculum periodically and evaluating its effectiveness.

f. Communicating key messages to all personnel in a timely fashion via a security awareness communication program.

g. Training all personnel initially and periodically thereafter (for example, annually).

While none of these baseline practices are specific to the CCS OB system security training, the emphasis and content for the training programs needs to show the relationship between the CCS OB system security and Health, Safety, and Environmental (HSE) consequences.

2.4.3.3 Additional practices

The following seven actions are additional practices:

a. Establishing cyber security training as a component of the company's overall training organization for all employees.

b. Tailoring the cyber security training curriculums with a progression of material for a given role in the organization.

c. Maintaining and reviewing records of employee training and schedules for training updates on a regular basis depending on their position/role.

d. Leveraging cyber security training provided by vendors.

e. Establishing the timing, frequency and content of the security awareness communication program in a document to enhance the organizations' understanding of cyber security controls.

f. Including an overview of the security awareness communication program for all personnel to ensure they are aware of the security practices on their first day.

g. Reviewing the training and the security awareness program annually for its effectiveness, applicability, content and consistency with tools currently used and corporate practices.

2.5 Interface with other Stakeholders (Engineering, Safety, RAM, V&V, T&C)

2.5.1 Overview

Common design reviews between

- the cybersecurity-team,
- the safety-team, and
- the design-team

shall be held to assess that proposed cybersecurity measures do not adversely impact

- the cybersecurity functions,
- the safety functions, or
- the operational functions

of the SuC on its development including but not limited to issues related to

- cost,
- operability,
- reliability,
- performances,
- etc.

To solve these issues, co-engineering between the cybersecurity-, safety-, and design-team is indispensable. In particular in safety risk analysis, hazards resulting from cybersecurity functions need to be identified by the safety-team which shall communicate them back to the cybersecurity-team. Here, the safety engineer shall support the cybersecurity-team in order to assess the safety implications of the cybersecurity functions on the

safety of the SuC during the cybersecurity assessment, but the derivation of appropriate cybersecurity measures that avoid impact on the safety of the SuC is the responsibility of the cybersecurity engineers in accordance with the cybersecurity standards.

2.5.2 Interfaces between Cybersecurity, Safety, and Design Processes

To ensure the necessary stability and viability of the design and safety-related documentation and approvals, the provision of cybersecurity, safety, and operational functionalities of the SuC shall be coordinated to decouple the different lifecycles and approval processes. This shall be achieved by communication and interaction between the cybersecurity-, safety- and design-team throughout the lifecycles and appropriate review processes via the synchronisation points defined in Figure 6 of the TS 50701 [11].

The safety-team shall provide, as input to the cybersecurity-team, information regarding the safety-related functions or assets to be protected. This information shall be documented and serves as an input to the cybersecurity risk assessment.

Conversely, the cybersecurity-team shall provide, as input to the safety-team, information regarding the cybersecurity-related functions or assets with an impact on the safety of the SuC. This information shall be documented and serves as an input to the safety risk assessment.

In the event that

- RAM-, safety- and cybersecurity-functional or non-functional requirements or
- Application Conditions (APs), Safety-Related Application Conditions (SRACs), and/or Security-Related Application Conditions (SecRACs)

are mutually incompatible or conflict with other SuC requirements such as, but not limited to RAM or performance requirements, relevant stakeholders shall cooperate to resolve the issue(s). The resolution of such conflicts

- must not involve a compromise regarding the fulfilment of any functional and/or technical safety requirement of the CCS or its subsystems.
- must in no way affect any existing evidences of functional and technical safety documented in the Safety Cases of existing CCSs and their subsystems.

All cybersecurity threats shall be entered into the threat-log and analysed regarding their impact on

- the cybersecurity resilience, and
- the safety

of the SuC and the results shall be documented in

- the threat-analysis and
- the hazard-analysis,

respectively.

To ensure the necessary stability and viability of safety-related documentation and approval, it is advisable to separate cybersecurity and safety issues as far as possible and coordinate them adequately in order to decouple the different lifecycles and the approval processes. Otherwise, each change affecting the security of the system may trigger a new safety approval. This is achieved, when cybersecurity threats or their defences affecting the safety of the SuC, the defences shall be changed until they no longer impact the safety of the SuC. This is necessary to prevent the CCS or any of its subsystems from losing its safety integrity, and thus its approval, due to a new cyber threat or its defence against it.

If cybersecurity threats have been identified having impact on the safety of the SuC, the cybersecurity case shall include or refer evidence on how cybersecurity threats with the potential to affect safety-related functions have been evaluated and how protection against adverse influence has been achieved. The cybersecurity case and its SecRACs shall be communicated to the safety manager for review and approval.

Figure 6 of the TS 50701 [11]defines the synchronisation, i.e. interfaces, between the cybersecurity-team and other stakeholders. It shows from left to right

1. the development phases in accordance with the EN 50126-1 [9],
2. the synchronisation points,

3. the provision and receipt of information among
    - the design / development team and others,
    - the safety-team, and
    - the cybersecurity-team.

2.6 Key Milestones

2.6.1 Phase-related Cybersecurity Activities

The key milestones mark the successful completion of the phases defined in the EN 50126-1 [9] for the railway application lifecycle. Table 2 from [11] defines the relevant

- security-related activities,
- necessary synchronisation points required to achieve coordination between the security activities and all the stakeholders (see also section 2.5), i.e. system engineering, safety, RAM, V&V, T&C activities, and
- deliverables to be exchanged

for the phases 0 through 5 of the cybersecurity-related railway application lifecycle in accordance with the TS 50701 [11].

Note

1. The phases 6 through 12 of the EN 50126-1 [9] are outside the scope of this document.

Phase (EN 50126-1 [9])		**Synchronisation Points and Deliverables**	**Cybersecurity Activities and Key Milestones (KMs)**
0	**Prerequisites**	----	**Activities** • Railway operator's "Security Program" (see Annex B in chapter 5) is established • Manufacturer's and integrator's secure development process is established • Legal and regulatory framework is identified • Start developing the "Security Program" (see Annex B in chapter 5) **Documentation** • Prepare "Identification of Legal and Regulatory Framework Report" • Start the specification of the "Security Program" (see Annex B in chapter 5) • Prepare "Cybersecurity End-of-Phase Verification Reports of Phase 0" (CSecEoPVerR_Phase 0) in accordance with section 2.6.2 ➔ **Key Milestone 0**
1	**Concept**	**SuC Identification**	**Activities**

Phase (EN 50126-1 [9])		Synchronisation Points and Deliverables	Cybersecurity Activities and Key Milestones (KMs)
		→ Operational environment incl. existing security-related controls and High-Level zone model (see chapter 4 in the TS 50701 [11]) → Applicable security standards → Purpose and scope ← Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities according Annex G, G.2 of the TS 50701 [11])	• Review of the level of security achieved up to now. • Analysis of the project's security implication and context (incl. generic threats) (see section 5.4 in the TS 50701 [11]). • Alignment with railway operator / asset owner and stakeholder's security goals. • Consideration of security lifecycle aspects (patch management, monitoring, etc.) (see chapter 10 in the TS 50701 [11]). • Continue developing the "Security Program" (see Annex B in chapter 5) • Document assets, services, and personnel needing some level of protection • Document potential internal and external threats to the enterprise • Establish security mission, visions, and values • Develop security policies for the CCS and equipment, information systems and personnel **Documentation** • Prepare "System Identification" • Prepare "Project Security Management Plan" • Continue the specification of the "Security Program" (see Annex B in chapter 5) • Prepare "Cybersecurity End-of-Phase Verification Reports of Phase 1" (CSecEoPVerR_Phase 1) in accordance with section 2.6.2 ➔ **Key Milestone 1**
2	**System definition and operational context**	**System Definition** → System boundaries → Initial system architecture, incl. list of functions, interfaces and generic systems → Logical and physical network plans ← Initial system architecture review, logical and physical network plans review **Operational Context and**	**Activities** • Review of the initial system architecture and of the logical and physical network plans. • Continue the development of the "Security Program" (see Annex B in chapter 5). • Define functional security requirements for the CCS zone and the CCS-Subsystem Zone. Potential activities and events are defined and documented to

Phase (EN 50126-1 [9])		Synchronisation Points and Deliverables	Cybersecurity Activities and Key Milestones (KMs)
		Criticality → Essential functions ← Initial risk analysis results ← Zones and Conduits	perform the functional requirements. • Define functional security organisation and structure. • Define functions required in the implementation plan. • Define and publish security zones, borders, and Access Control (AC) portals. • Complete and issue security policies, and procedures. • Establish the planning documents. • ** Initial Risk Assessment (IRA) for the SuC (see section 6.3 in the TS 50701 [11])* • ** Partitioning of the SuC into Zones and Conduits (see section 6.4 in the TS 50701 [11])* • ** Documentation of components, interfaces and characteristics for each Zone and Conduit (see section 6.5 in the TS 50701 [11])* **: This activity and the corresponding synchronisation point may also be conducted in phase 3.* **Documentation** • Prepare “Cybersecurity Quality Assurance Plan” • Prepare “Cybersecurity Quality Assurance Verification Report” • Prepare “Cybersecurity Configuration Management Plan” • Prepare “Incident Response Plan” • Continue the specification of the “Security Program” (see Annex B in chapter 5) • Prepare “Cybersecurity Verification Plan” • Prepare “Cybersecurity Validation Plan” • Prepare “System Definition” • Prepare “Operational Context and Criticality Report” • Prepare “Cybersecurity End-of-Phase Verification Reports of Phase 2” (CSecEoPVerR_Phase 2) in accordance with section 2.6.2

Phase (EN 50126-1 [9])		Synchronisation Points and Deliverables	Cybersecurity Activities and Key Milestones (KMs)
			➔ **Key Milestone 2**

3	**Risk analysis and evaluation**	**Detailed Risk Assessment (DRA)**
		→ Functional Requirements (linked to essential functions)
		← Initial Threat Log
		← Potential updates (Zones and Conduits, network plans)
			Activities
			• Detailed Risk Assessment (DRA) (see chapter 7 in the TS 50701 [11]) covering, e.g.
			  ○ Perform a risk analysis of potential vulnerabilities and threats
			  ○ Perform vulnerability assessment of facilities and associated services against the list of potential threats
			  ○ Categorise risks, potential impacts to the enterprise, and potential mitigations
			• Continue the development of the "Security Program" (see Annex B in chapter 5)
			• Derive technical (e.g. SL-T), physical and organizational countermeasures or assumptions for Zones and Conduits
			• Consider business continuity aspects (incl. incidence response and recovery) for the SuC
			
			Documentation
			• Prepare "Detailed Risk Assessment Report"
			• Continue the specification of the "Security Program" (see Annex B in chapter 5)
			• Prepare "Cybersecurity End-of-Phase Verification Reports of Phase 3" (CSecEoPVerR_Phase 3) in accordance with section 2.6.2
			
			➔ **Key Milestone 3**

4	**Specification of system requirements**	**Cybersecurity Requirements Specifications (CRS) Release**
		← System CRS incl. Security-Related Application Conditions (SecRACs)
			Activities
			• SuC-specific refinement of normative requirements (see chapter 8 in the TS 50701 [11])
			• Specify the Cybersecurity Requirements covering, e.g.
			  ○ Establish security functional requirements for the CCS and equipment, production systems, information systems, and personnel
			  ○ Segment security work into controllable tasks and

Phase (EN 50126-1 [9])		Synchronisation Points and Deliverables	Cybersecurity Activities and Key Milestones (KMs)
			modules for development of functional designs ○ Establish network functional definitions for security portions of the CCS • Continue the development of the "Security Program" (see Annex B in chapter 5) • Definition of organisational and physical requirements • Definition of SecRACs (see chapter 7 in the TS 50701 [11]) **Documentation** • Prepare "Cybersecurity Requirements Specification" • Prepare "Overall Cybersecurity Test Specification" • Continue the specification of the "Security Program" (see Annex B in chapter 5) • Prepare "Cybersecurity End-of-Phase Verification Reports of Phase 4" (CSecEoPVerR_Phase 4) in accordance with section 2.6.2 • Prepare "Cybersecurity Validation Reports of Phase 4" (CSecValR_Phase 4) in accordance with section ➔ **Key Milestone 4**
5	**Architecture and apportionment of system requirements**	**CRS breakdown:** → System architecture breakdown to subsystem and components, incl. SuC inventory ← Subsystem Cybersecurity Requirements Specification incl. security-related application conditions, technical and organizational compensating countermeasures	**Activities:** • DRA update, incl. assessment of the SL-C for components and definition of compensating countermeasures including security-related application condition (see chapter 8.3 in the TS 50701 [11]) • Assigning the technical security requirements to components and conduits (see chapter 8.3 in the TS 50701 [11]) • Assigning responsibilities for the organizational and physical requirements for the railway operator/maintainer or asset owner • Establish third party management for security aspects, including supplier security capabilities and support contracts

Phase (EN 50126-1 [9])		Synchronisation Points and Deliverables	Cybersecurity Activities and Key Milestones (KMs)
			Documentation • Create the Cybersecurity CCS Architecture (incl. network architecture, network segment architecture (if required), assets, security zones) Specification of CCS subsystems and components • Create Cybersecurity CCS Design Specification of CCS subsystems and components • Create Cybersecurity CCS Interface Specification of CCS subsystems and components • Create Cybersecurity CCS Software Integration Test Specification of CCS subsystems and components • Create Cybersecurity CCS Hardware/Software Integration Test Specification of CCS subsystems and components • Update Security Validation Plan (if appropriate) • Update Security-Related Application Conditions (SecRACs) (if appropriate) • Update Detailed Risk Assessment Report (if appropriate) • Continue the specification of the “Security Program” (see Annex B in chapter 5) • Prepare “Cybersecurity End-of-Phase Verification Reports of Phase 5” (CSecEoPVerR_Phase 5) in accordance with section 2.6.2

Table 2: Security-related Activities within a Railway Application Lifecycle specified in the EN 50126-1 [9]

2.6.2 Cybersecurity Verification

2.6.2.1 General

The cybersecurity verification tasks shall be performed at the end of each lifecycle phase listed in Table 2.

The cybersecurity verification shall demonstrate that the cybersecurity requirements of the related lifecycle phase have been fulfilled. For this purpose, the cybersecurity verification tasks shall demonstrate

1. the correctness and adequacy of the security risk assessment, where specified.
2. the compliance of the cybersecurity deliverables of the phase with the cybersecurity deliverables of the former phase.
3. the adequate prevention of the identified cybersecurity risks by the specified Cybersecurity

Requirements Specification (CSR).

4. the adequacy of the specified methods, tools and techniques used within the lifecycle phase, where specified.
5. the correctness, consistency, and adequacy of test specifications and executed tests, as appropriate.

Errors or deficiencies identified in the process of the cybersecurity verification of a phase may require the re-application of some or all activities of one or more previous lifecycle phases.

2.7 Communication and Reporting

2.7.1 Role Related Reporting Rules

The role related reporting rules are defined in section 2.2 and project organisation chart provided in Figure 1.

2.7.2 Incident Planning and Response

2.7.2.1 Objective

Predefine how the organization will detect and react to cyber security incidents.

2.7.2.2 Description

When developing a program for incident planning and response, it is important to include all systems in scope and not just limit the effort to traditional computer room facilities. Part of the incident response plan should include procedures for how the organization will respond to incidents, including notification and documentation methods, investigations, recoveries and subsequent follow-up practices.

2.7.2.3 Rationale

Identifying an incident early and responding appropriately can limit the consequences of the event. Incident planning and response provides the organization the opportunity to plan for security incidents and then to respond according to the established company practices. No matter how much care is taken in protecting a system, it is always possible that unwanted intrusions might compromise the system. Technology vulnerabilities continue to exist, and external threats are increasing in number and sophistication, therefore requiring a robust strategy for determining the appropriate planning and response. Insight gained from actual incidents is captured because it is critical for evaluating and improving the Cyber-Security Management System (CSMS).

2.7.2.4 Requirements

The “Incident Response Plan” shall be created.

2.7.3 Classify, Manage, Safeguard, and Present Information at Appropriate Time to Authorised Personnel

2.7.3.1 Objective

Classify, manage, safeguard and present the information associated with the CCS and “Security Program” at the appropriate time to authorized personnel.

2.7.3.2 Description

Organizations should employ comprehensive information and document management policies for information assets within the scope of their CCS and “Security Program”. Care should be given to protect this information and verify that the appropriate versions are retained. Information classification systems that allow information assets to receive the appropriate level of protection are the key to meet this objective.

2.7.3.3 Rationale

Much of the information about the CCS may be stored electronically or in hardcopy outside the CCS and is not protected by CCS authorization controls. Unauthorized access and use of this information are threats to CCS security. This information needs to be appropriately controlled and managed.

2.7.3.4 Requirements

The requirements for the information and document management shall cover the topics listed in Table 3.

ID	Description	Requirement
1	Develop lifecycle management processes for the CCS information	A lifecycle document management process shall be developed and maintained for the CCS information.
2	Define information classification levels	Information classification levels (for example, company confidential, restricted and public) shall be defined for access and control, including sharing, copying, transmitting, and distributing appropriate for the level of protection required.
3	Classify all “Security Program” information assets	All logical assets within the scope of the CCS (that is, control system design information, vulnerability assessments, network diagrams and industrial operations programs) shall be classified to indicate the protection required appropriate with the consequence of its unauthorised disclosure or modification.
4	Ensure appropriate records control	Policies and procedures shall be developed detailing retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.
5	Ensure long-term records retrieval	Appropriate measures shall be employed to ensure long-term records can be retrieved (that is, converting the data to a new format or retaining older equipment that can read the data).
6	Maintain information classifications	Information that requires special control or handling shall be reviewed on a periodic basis to validate that special handling is still required.
7	Audit the information and document management process	Periodic reviews of compliance to the information and document management policy shall be performed.

Table 3: Requirements for the Information and Document Management

3 Cybersecurity Context

3.1 High Level Description of the System under Consideration (SuC)

The document is a generic description of PSMP that can be used as a template if the approval process of a formally project is started. Therefore, the high-level description of the system under consideration (SuC) is not defined here.

The system under consideration (SuC) is defined in the OCORA Security Concept [8].

3.2 Cybersecurity Objectives

The cybersecurity objectives are:

- Development of a secure architecture based on IEC 62443 and TS 50701 requirements
- Taking into account life-cycle security, software-update and maintenance activities
- Develop a cybersecurity strategy to maintain the security status of the lifetime of the system/product

3.2.1 Basic Cybersecurity Strategy Elements

3.2.1.1 Avoiding attacks

One approach to avoid the threats is to reduce the attack surface. This about the digital economy of data. Generate as little data as possible and as much as necessary. Furthermore, not all systems should be connected to the internet.

Prefer to not use technologies, products and services that have known vulnerabilities. For example, implement a two-vendor strategy for software products. This means, if a vulnerability becomes known, the alternative software can be used.

Avoiding attacks is the best security strategy, but this can only be implemented to a limited extent if the connectivity possibilities with all its advantages want to be used.

3.2.1.2 Prevention attacks

This is the most used security strategy.

Use cyber security mechanisms that provide a high impact against attacks to protect the systems and data worth protecting.

Examples:

Use of encryption (file-, hard disk-, email encryption, VPN systems, SSL/TLS). Use of Authentication procedures (Challenge-Response, Global Identity, etc.). Proactive software updates / patches.

3.2.1.3 Detecting attacks

If the cyber security precautions could not prevent the attacks, the attacks must be detected as quickly as possible, and the damage must be kept as small as possible.

The development of a concept to monitor and check the attacks on the part of clients, servers and network traffic is imperative.

3.2.1.4 Build an understanding of what is worth protecting

To determine which systems and data are important, a protection needs analysis must be done.

3.2.2 Cyber security requirements

The cyber security requirements are derived in iterative steps based on the process definition of IEC 62443 and TS 50701. The process is defined in the coordinated Cyber Security Guideline [7].

The results of the analysis are presented in the phase related documents. These are:

- Phase 2: Cyber Security Concept [8]
- Phase 3: Cyber Security Threat and Risk Analysis (for later release)
- Phase 4: Cyber Security System Requirements (for later release)
- Phase 5: Cyber Security Component Requirements (for later release)

3.3 Available Cybersecurity Regulations and Standards

3.3.1 Regulations

The European Cybersecurity Regulations are listed in Table 4.

ID	Title
	European Cybersecurity Regulation
Regulation (EU) 2016/679	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27. April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)2022/0084 2022/0084
Regulation (EU) 2019/0001 (*Proposal, COM(2019) 3 final*)	Regulation of the European Parliament and of the Council Establishing the Conditions for Accessing the other EU Information Systems and Amending Regulation (EU) 2018/1862 and Regulation (EU) yyyy/xxxx
Regulation (EU) 2022/0085 (*Proposal, COM(2022 122 final*)	Regulation (EU) 2022/0085 of the European Parliament and of the Council on Information Security in the Institutions, Bodies, Offices and Agencies of the Union

Table 4: European Cybersecurity Regulations

3.3.2 Standards

3.3.2.1 RAMS Standards

The RAMS standards are listed in Table 5.

ID	Title
	RAMS Process related Standards
EN 50126-1	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
EN 50126-2	Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
	Software related Standards
EN 50128	Railway applications – Communication, signalling and processing systems - Software for railway control and protection systems
EN 50657	Railways Applications – Rolling stock applications – Software on Board Rolling Stock

ID	Title
	Hardware & Approval related Standard
EN 50129	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
	Communication related Standards
EN 50159	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems
IEC 62784-3	Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions

Table 5: RAMS Standards

3.3.2.2 Cybersecurity Standards

The available cyber security standards are listed in Table 6, Table 7, Table 8 and Table 9. They are grouped as follows:

1. CENELEC cybersecurity Technical Specification (TS) is listed in Table 6.
2. IEC cybersecurity standards are listed in Table 7.
3. ISO cybersecurity standards are listed in Table 8.
4. NIST Special Publications (SP) are listed in Table 9.

For cybersecurity in railway applications the standard in Table 6 is the leading one.

ID	Title
	General
TS 50701	Railway Applications - Cybersecurity

Table 6: CENELC Cybersecurity Technical Specification (TS)

ID	Title
	General
IEC 62443-1-1	Industrial Communication Networks – Network and System Security - Part 1-1: Terminology, Concepts and Models
IEC 62443-1-2	*Industrial Communication Networks – Network and System Security - Part 1-2: Master Glossary of Terms and Abbreviations*
IEC 62443-1-3	*Industrial Communication Networks – Network and System Security - Part 1-3: System Security Compliance Metrics*
IEC 62443-1-4	*Industrial Communication Networks – Network and System Security - Part 1-4: IACS Security Lifecycle and Use Case*
	Policies and Procedures
IEC 62443-2-1	Industrial Communication Networks – Network and System Security - Part 2-1: Establishing an Industrial Automation and Control System Security Program
IEC 62443-2-2	*Security for Industrial Automation and Control Systems - Part 2-2: Implementation Guidance for an IACS Security Management System*
IEC 62443-2-3	Security for Industrial Automation and Control Systems - Part 2-3: Patch Management in the IACS Environment
IEC 62443-2-4	Security for Industrial Automation and Control Systems - Part 2-4: Security Program Requirements for IACS Service Providers

ID	Title
IEC 62443-2-5	*Part 2-5: Implementation Guidance for IACS Asset Owners*
	System
IEC 62443-3-1	Industrial Communication Networks – Network and System Security - Part 3-1: Security Technologies for Industrial Automation and Control Systems
IEC 62443-3-2	Industrial Communication Networks – Network and System Security - Part 3-2: Security Risk Assessment for System Design
IEC 62443-3-3	Industrial Communication Networks – Network and System Security - Part 3-3: System Security Requirements and Security Levels
	Component and Products
IEC 62443-4-1	Security for Industrial Automation and Control Systems - Part 4-1: Secure Product Development Lifecycle Requirements
IEC 62443-4-2	Security for Industrial Automation and Control Systems - Part 4-2: Technical Security Requirements for IACS Components

Table 7: IEC Cybersecurity Standards (standards in italics are not yet available (n.y.a.))

ID	Title
	Security Management System – Overview & Vocabulary
ISO 27000	Information Technology – Security Techniques - Information Security Management Systems – Overview and Vocabulary
	Security Management System Requirements
ISO 27001	Information Technology – Security Techniques – Information Security Management Systems - Requirements
	Security Controls
ISO 27002	Information Security – Cybersecurity and Privacy Protection - Information Security Controls
	Risk Management
ISO 27005	Information Technology – Security Techniques - Information Security Risk Management

Table 8: ISO Cybersecurity Standards

ID	Title
	Introduction to Information Security
NIST SP 800-12	An Introduction to Information Security
	Developing Security Plans
NIST SP 800-18	Guide for Developing Security Plans for Federal Information Systems
	Security Risks & Risk Assessments
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-39	Managing Information Security Risks

ID	Title
	Security and Privacy Controls
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
	System Security Engineering
NIST SP 800-160A	System Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
NIST SP 800-160B	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

Table 9: NIST Cybersecurity Special Publications

4 Annex A: Key Cybersecurity Roles and Responsibilities

This Annex defined the key cybersecurity roles and responsibilities in the subsequent tables:

- Table 10: Requirements Manager (RQM)
- Table 11: Designer (DES)
- Table 12: Implementer (IMP)
- Table 13: Tester (TST)
- Table 14: Integrator (INT)
- Table 15: Verifier (VER)
- Table 16: Validator (VAL)
- Table 17: Assessor (ASR)
- Table 18: Project Manager (PM)
- Table 19: Configuration Manager (CM)
- Table 20: System / security Administrator (SAD)

Role: Requirements Manager (RQM)
Responsibilities: 1. shall be responsible for specifying the cybersecurity requirements. 2. shall own the Cybersecurity Requirements Specification. 3. shall establish and maintain traceability to and from system level cybersecurity requirements. 4. shall ensure the cybersecurity specifications and cybersecurity requirements are under change and configuration management including state, version and authorisation status. 5. shall ensure consistency and completeness in the Cybersecurity Specification (with reference to user requirements and final environment of application). 6. shall develop and maintain the cybersecurity requirement documents.
Key competences: 1. shall be competent in cybersecurity requirements engineering. 2. shall be experienced in cybersecurity application's domain. 3. shall be experienced in cybersecurity attributes of cybersecurity application's domain. 4. shall understand the overall role of the system and the environment of application. 5. shall understand analytical techniques and outcomes. 6. shall understand applicable cybersecurity regulations. 7. shall understand the cybersecurity requirements of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 10: Requirements Manager (RQM)

Role: Designer (DES)
Responsibilities: 1. shall transform specified cybersecurity requirements into acceptable cybersecurity solutions. 2. shall own the architecture and downstream cybersecurity solutions. 3. shall define or select the design methods and supporting tools. 4. shall apply appropriate design principles and cybersecurity standards. 5. shall develop component cybersecurity specifications where appropriate.

6. shall maintain traceability to and from the specified cybersecurity requirements. 7. shall develop and maintain the cybersecurity design documentation. 8. shall ensure cybersecurity design documents are under change and configuration control.
Key competences: 1. shall be competent in engineering appropriate to the cybersecurity application area. 2. shall be competent in cybersecurity design principles. 3. shall be competent in design analysis & design test methodologies. 4. shall be able to work within design constraints in a given cybersecurity environment. 5. shall be competent in understanding the cybersecurity problem domain. 6. shall understand all the constraints imposed by the hardware platform, the operating system and the interfacing systems. 7. shall understand the relevant parts of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 11: Designer (DES)

Role: Implementer (IMP)
Responsibilities: 1. shall transform the cybersecurity design solutions into data/source code/other design representations. 2. shall transform cybersecurity source code into executable code/other design representation. 3. shall apply cybersecurity design principles. 4. shall apply specified cybersecurity-related data preparation/coding standards. 5. shall carry out analysis to verify the intermediate outcome. 6. shall integrate cybersecurity functions and cybersecurity barriers on the target machine. 7. shall develop and maintain the implementation documents comprising the applied methods, data types, and listings. 8. shall maintain traceability to and from design. 9. shall maintain the generated or modified data/code under change and configuration control.
Key competences: 1. shall be competent in engineering appropriate to the cybersecurity application area. 2. shall be competent in the implementation language and supporting tools. 3. shall be capable of applying the specified cybersecurity coding standards and cybersecurity programming styles. 4. shall understand all the constraints imposed by the hardware platform, the operating system and the interfacing systems. 5. shall understand the relevant parts of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 12: Implementer (IMP)

Role: Tester (TST)
Responsibilities: 1. shall ensure that cybersecurity test activities are planned. 2. shall develop the cybersecurity test specification (objectives & cases). 3. shall ensure traceability of test objectives against the specified cybersecurity requirements and of

test cases against the specified test objectives. 4. shall ensure that the planned cybersecurity tests are implemented and specified tests are carried out. 5. shall identify deviations from expected results and record them in test reports. 6. shall communicate deviations with relevant change management body for evaluation and decision. 7. shall capture outcomes in cybersecurity reports. 8. shall select the test equipment.
Key competences: 1. shall be competent in the domain where testing is carried out e.g. cybersecurity requirements, data, code etc. 2. shall be competent in various test and verification approaches / methodologies and be able to identify the most suitable method in a given cybersecurity context. 3. shall be capable of deriving test cases from given cybersecurity specifications. 4. shall have analytical thinking ability and good observation skills. 5. shall understand the relevant parts of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 13: Tester (TST)

Role: Integrator (INT)
Responsibilities: 1. shall manage the cybersecurity integration process using the cybersecurity baselines. 2. shall develop the Cybersecurity Integration Test Specification, Cybersecurity Software/Hardware Integration Test Specification and the Cybersecurity Barrier Integration Test Specification for cybersecurity components based on the Designer's cybersecurity component specifications and cybersecurity architecture stating what the necessary input components, the sequence of integration activities and the resultant integrated components are. 3. shall develop and maintain records on the cybersecurity integration activities. 4. shall identify integration anomalies, record and communicate these to relevant change management body for evaluation and decision making. 5. shall develop a cybersecurity component and overall system integration report stating the outcome of the cybersecurity integration.
Key competences: 1. shall be competent in the domain where cybersecurity component integration is carried out, e.g. relevant programming languages, cybersecurity function interfaces, cybersecurity barrier, operating systems, data, platforms, code, etc. 2. shall be competent in various cybersecurity integration approaches/methodologies and be able to identify the most suitable method or combination of methods in a given cybersecurity context. 3. shall be competent in understanding the design and cybersecurity functionality required at various intermediate levels. 4. shall be capable of deriving the types of cybersecurity integration test from a set of integrated cybersecurity functions and integrated cybersecurity barriers. 5. shall have analytical thinking ability and good observation skills tending towards the system level perspective. 6. shall understand the relevant parts of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 14: Integrator (INT)

Role: Verifier (VER)
Responsibilities: 1. shall develop a Cybersecurity Verification Plan (which may include quality issues) stating what needs verification and what type of process (e.g. review, analysis etc.) and test is required as evidence. 2. shall check the adequacy (completeness, consistency, correctness, relevance and traceability) of the documented evidence from review, integration and testing with the specified verification objectives. 3. shall identify anomalies, evaluate these in risk (impact) terms, record and communicate these to relevant change management body for evaluation and decision. 4. shall manage the verification process (review, integration and testing) and ensure independence of activities as required. 5. shall develop and maintain records on the verification activities. 6. shall develop a Cybersecurity Verification Report stating the outcome of the verification activities.
Key competences: 1. shall be competent in the domain where verification is carried out e.g. cybersecurity requirements, data, code etc. 2. shall be competent in various verification approaches/methodologies and be able to identify the most suitable method or combination of methods in a given cybersecurity context. 3. shall be capable of deriving the types of verification from given cybersecurity specifications. 4. shall have analytical thinking ability and good observation skills. 5. shall understand the relevant parts of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 15: Verifier (VER)

Role: Validator (VAL)
Responsibilities: 1. shall develop a system understanding of the cybersecurity within the intended environment of application. 2. shall develop a Cybersecurity Validation Plan and specify the essential tasks and activities for cybersecurity validation and agree this plan with the assessor. 3. shall review the cybersecurity requirements against the intended environment/use. 4. shall review the cybersecurity functions and cybersecurity barriers against the cybersecurity requirements to ensure all of these are fulfilled. 5. shall evaluate the conformity of the cybersecurity process and the developed cybersecurity functions and cybersecurity barriers against the cybersecurity requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20] including the assigned SL. 6. shall review the correctness, consistency and adequacy of the verification and testing. 7. shall check the correctness, consistency and adequacy of test cases and executed tests. 8. shall ensure all Cybersecurity Validation Plan activities are carried out. 9. shall review and classify all deviations in terms of risk (impact), records and submits to the body responsible for Change Management and decision making. 10. shall give a recommendation on the suitability of the cybersecurity functions and cybersecurity barriers for intended use and indicate any application constraints as appropriate. 11. shall capture deviations from the Cybersecurity Validation Plan. 12. shall carry out audits, inspections or reviews on the overall project (as instantiations of the generic development process) as appropriate in various phases of development. 13. shall review and analyse the Cybersecurity Validation Reports relating to previous applications as

appropriate. 14. shall review that the developed solutions are traceable to the cybersecurity requirements. 15. shall ensure the related threat logs and remaining non-conformities are reviewed and all threads closed out in an appropriate manner through elimination or risks control/transfer measures. 16. shall develop a Cybersecurity Validation Report. 17. shall give agreement/disagreement for the release of the cybersecurity functions and cybersecurity barriers.
Key competences: 1. shall be competent in the domain where cybersecurity validation is carried out. 2. shall be experienced in cybersecurity attributes of cybersecurity application's domain. 3. shall be competent in various validation approaches/methodologies and be able to identify the most suitable method or combination of methods in a given cybersecurity context. 4. shall be capable of deriving the types of validation evidence required from given cybersecurity specifications bearing in mind the intended application. 5. shall be capable of combining different sources and types of evidence and synthesise an overall view about fitness for purpose or constraints and limitations of the application. 6. shall have analytical thinking ability and good observation skills. 7. shall have overall cybersecurity understanding and perspective including understanding the application environment. 8. shall understand the requirements of the TS 50701 [11] and IEC 63443 series [12] to [20].

Table 16: Validator (VAL)

Role: Assessor (ASR)
Responsibilities: 1. shall develop a system understanding of the cybersecurity within the intended environment of application. 2. shall develop an Cybersecurity Assessment Plan and communicate this with the cybersecurity authority and the client organisation (contracting body of the assessor). 3. shall evaluate the conformity of the cybersecurity process and the developed cybersecurity functions and cybersecurity barriers against the cybersecurity requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20] including the assigned SL. 4. shall evaluate the competency of project staff and organisation for the cybersecurity development. 5. shall evaluate the verification and validation activities and the supporting evidence. 6. shall evaluate the quality management systems adopted for the development. 7. shall evaluate the configuration and change management system and the evidence of its use and application. 8. shall identify and evaluate in terms of risk (impact) any deviations from the cybersecurity requirements in the Cybersecurity Assessment Report. 9. shall ensure that the Cybersecurity Assessment Plan is implemented. 10. shall carry out cybersecurity audits and cybersecurity inspections on the overall cybersecurity development process as appropriate at various phases of the cybersecurity development. 11. shall give a professional view on the fitness of the developed cybersecurity functions and cybersecurity barriers for its intended use detailing any constraints, application conditions and observations for risk control as appropriate. 12. shall develop a Cybersecurity Assessment Report and maintain records on the cybersecurity assessment process.

Key competences:

1. shall be competent in the domain/technologies where cybersecurity assessment is carried out.
2. shall have acceptance/licence from a recognised cybersecurity authority.
3. shall have/strive to continually gain sufficient levels of experience in the cybersecurity principles and the cybersecurity application of the cybersecurity principles within the application domain.
4. shall be competent to check that a suitable method or combination of methods in a given cybersecurity context have been applied.
5. shall be competent in understanding the relevant cybersecurity, human resource, technical and quality management processes in fulfilling the cybersecurity requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20].
6. shall be competent in cybersecurity assessment approaches/methodologies.
7. shall have analytical thinking ability and good observation skills.
8. shall be capable of combining different sources and types of evidence and synthesise an overall view about fitness for purpose or constraints and limitations on cybersecurity application.
9. shall have overall cybersecurity understanding and perspective including understanding the cybersecurity application environment.
10. shall be able to judge the adequacy of all cybersecurity development processes (like quality management, configuration management, validation and verification processes).
11. shall understand the requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20]..

Table 17: Assessor (ASR)

Role: Project Manager (PM)

Responsibilities:

1. shall ensure that the quality management system and independency of roles according to 2.2 are in place for the project and progress is checked against the cybersecurity plans.
2. shall allocate sufficient number of competent resources in the project to carry out the essential tasks including cybersecurity activities, bearing in mind the requisite independence of roles.
3. shall ensure that a suitable validator has been appointed for the project as defined in the TS 50701 [11] and the IEC 62443 series [12] to [20].
4. shall be responsible for the delivery and deployment of the cybersecurity functions and cybersecurity barriers and ensure that cybersecurity requirements from the stakeholders are also fulfilled and delivered.
5. shall allow sufficient time for the proper implementation and fulfilment of cybersecurity tasks.
6. shall endorse partial and complete deliverables from the cybersecurity development process.
7. shall ensure that sufficient records and traceability is maintained in cybersecurity related decision making.

Key competences:

1. shall understand quality, competencies, organisational and management requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20].
2. shall understand the cybersecurity requirements of the cybersecurity process.
3. shall be able to weigh different options and understand the impact on cybersecurity performance of a decision or selected options.
4. shall understand the cybersecurity requirements of the cybersecurity development process.
5. shall understand the cybersecurity requirements of other relevant standards.

Table 18: Project Manager (PM)

Role: Configuration Manager (CM)
Responsibilities: 1. shall be responsible for the Cybersecurity Configuration Management Plan. 2. shall own the Cybersecurity Configuration Management System. 3. shall establish that all cybersecurity components are clearly identified and independently versioned inside the Cybersecurity Configuration Management System. 4. shall prepare Release Notes which includes incompatible versions of cybersecurity components.
Key competences: 1. shall be competent in cybersecurity configuration management. 2. shall understand the cybersecurity requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20].

Table 19: Configuration Manager (CM)

Role: System / security Administrator (SAD)
Responsibilities: 1. shall be responsible for the cybersecurity of all electronic data and data collecting, exchanging, processing and storing electronic devices used by any personnel of the project. 2. shall own all electronic data and data collecting, exchanging, processing and storing electronic devices used by any personnel of the project. 3. shall establish that all electronic data and data collecting, exchanging, processing and storing electronic devices used by any personnel of the project are clearly identified.
Key competences: 1. shall be competent in system cybersecurity management. 2. shall have strong familiarity with the operating system and its networking components; 3. shall have good understanding of the application and its environmental prerequisites; 4. shall have awareness of how the patch should interact with the application and operating system and what the possible consequences of the upgrade may be; and 5. shall have monitoring capabilities of the operation of the CCS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried. 6. shall understand the cybersecurity requirements of the TS 50701 [11] and the IEC 62443 series [12] to [20].

Table 20: System / security Administrator (SAD)

5 Annex B: Guidelines for the Development of the “Security Program”

5.1 Overview

The “security Program” is a documented set of

- policies,
- procedures,
- guidelines,
- requirements, and
- standards

that together provide protection against cyberattacks. This set of practices needs continuous further development and adaptation to align the protection with the ever development of the threat environment.

Guidance and requirements to establish and continuously further the development of the “Security Program” are provided for

- the CCS in section 5.2 and
- CCS service providers in section 5.3.

5.2 Guidance and Requirements to Establish the Security Program for the CCS

The “Security Program” of the CCS shall include the subsequent main categories to protect it against cyberattacks.

1. Risk analysis,
2. Addressing risk with the “Security Program”, and
3. Monitoring and improving the “Security Program”.

These categories are further divided into element groups and their associated elements depicted in Figure 2.

Detailed guidelines and requirements suited to establish the initial version and the continued further development of the “Security Program” for the CCS are provided in the IEC 62443-2-1 [13].

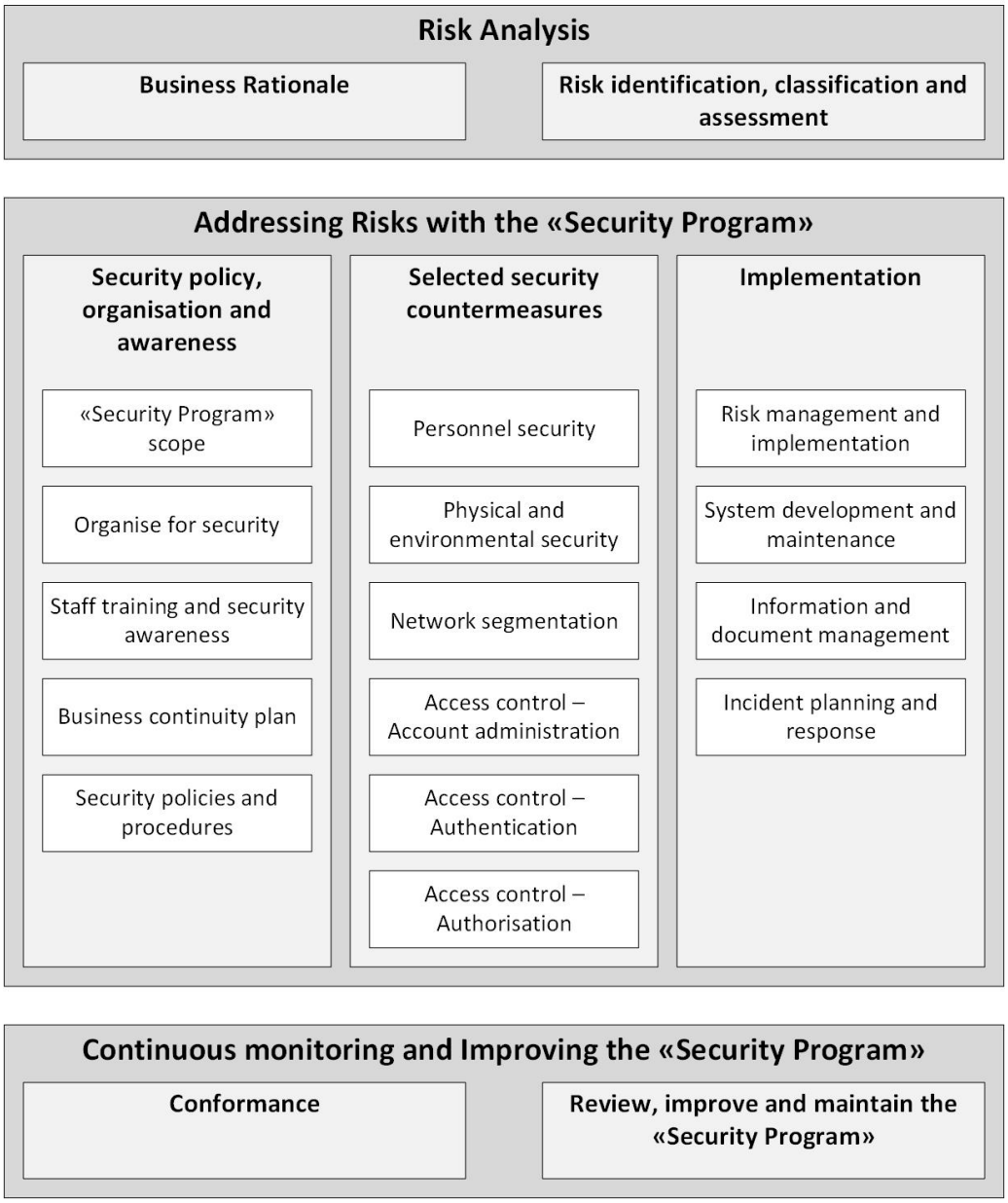

Figure 2: Element groups and their associated elements of the “Security Program”

5.3 Guidance and Requirements to Establish the “Security Program” for a CCS Service Provider

This section focuses on the set of requirements for security capabilities of CCS service providers they can offer to asset owners during integration and maintenance activities of the CCS.

Figure 3 illustrates how the integration and maintenance capabilities relate to the CCS and its “CCS Solution” which consists of the CCS’s subsystems and their equipment. Some of these capabilities reference security measures defined in the IEC 62443-3-3 [18] that the CCS service provider must ensure are supported in the “CCS Solution”.

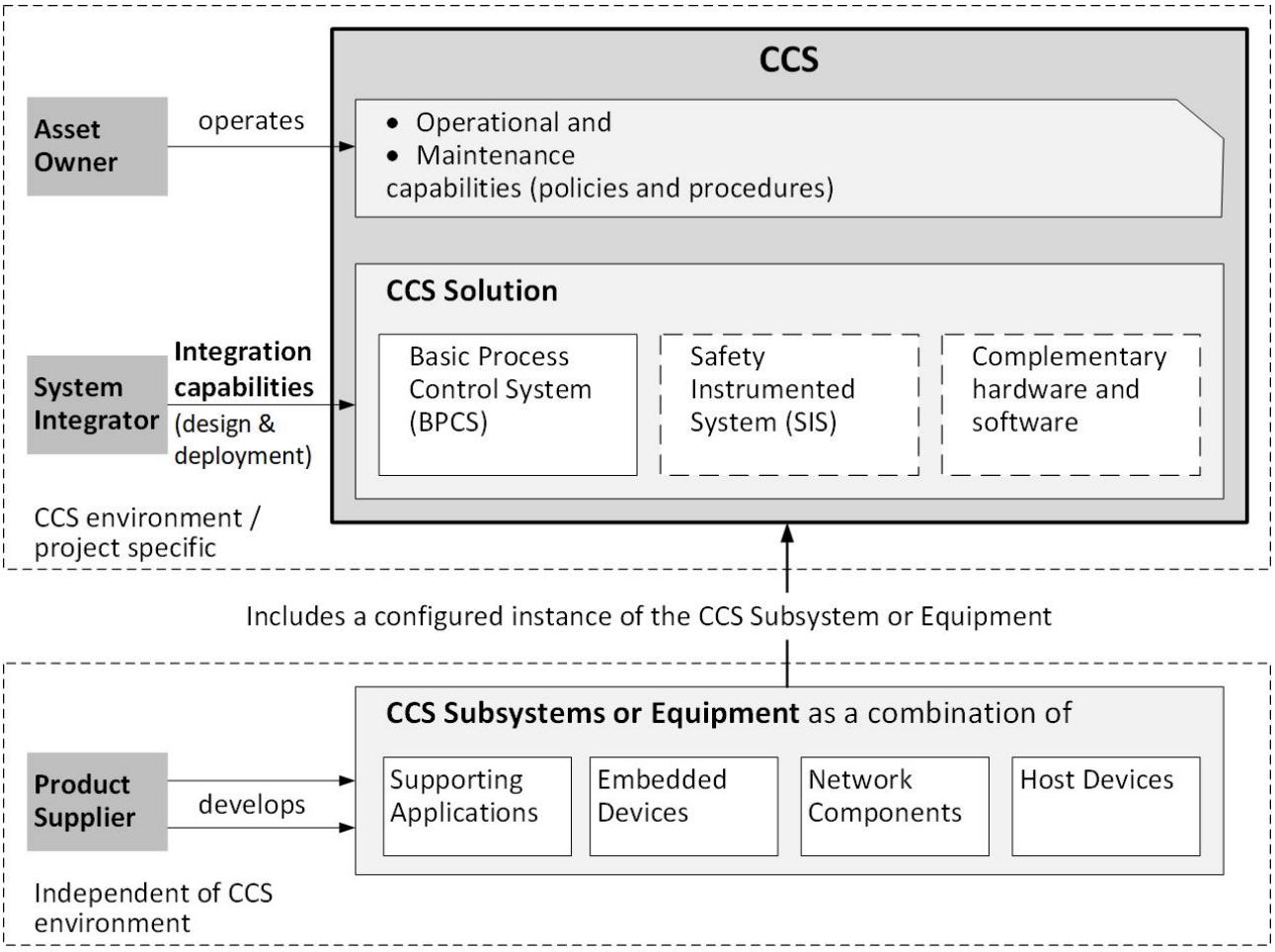

Figure 3: Scope of CCS service provider capabilities

Figure 3 illustrates the “CCS Solution” containing

- the Basic Process Control System (BPCS),
- the Safety Instrumented System (SIS), and
- optional supporting applications such as advanced control containing complementary hard- and software.

The dashed boxes indicate that these components are “optional”.

Detailed guidelines and requirements to create the initial version and continued further development of the “Security Program” for CCS service provider are provided in the IEC 62443-2-4 [15].