OCORA

Open CCS On-board Reference Architecture

RAMSS Policy

Document ID: OCORA-TWS07-203

Version: 1.00

Date: 26.06.2023

1 Management Summary

This document is established by the Technical Work-Stream TWS07 of the Open Control-Command and Signalling (CCS) Onboard Reference Architecture (OCORA) , based on the need for having an integral approach covering both RAMS domains and RAMS-related domains in the specification phase of CCS systems.

This document and the Policy in particular covers the following functional and non-functional domains, but might be extended in a future release of this Policy:

- System functions,
- Safety functions,
- Security functions,
- Communication functions,
- Reliability, Availability, Maintainability (RAM),
- Human Factors, and
- External influences.

The purpose of this document is threefold. First, in Chapter 2 it intends to clarify the relationships and potential related issues between functional and non-functional domains as listed above. Secondly, in Chapter 3 the explanation in this document helps the reader to understand, feel the urgency and help to acknowledge in which phase during the lifecycle of systems these conflicts and challenges may arise. And thirdly, forming the main part of this document in Chapter 4, to give clear principles, guidance and direction by providing a Policy for resolving these conflicts.

The Policy complies to the generic development process described in the EN 50126-1: 2017 [1] and is suited to resolve conflicts between RAMS and RAMS-related domains. This is of utmost importance as compromises on specific requirements and targets lead to unnecessary and difficult discussions, e.g.:

- the railway operators and infrastructure managers are not keen on accepting compromises on quality, reliability, availability, maintainability and system functions or capabilities,
- the railway safety authorities are not keen on accepting compromises on safety, and
- the railway security authorities are not keen on accepting compromises on security.

The policy, when used at the CENELEC development phases for Railway Applications, ensures that:

- requirements on higher aggregated level will be fulfilled, ensuring (higher) Availability and Reliability targets,
- additional costs due to necessary modifications at a later phase are avoided, and/or
- the original project planning will be achieved, without the need for conflict resolution, reiteration of the development phases or accepting concessions on the scope

which provides benefits for Railway Undertakers, Maintainers, Infrastructure Managers, OEMs, (Sub)Suppliers and specialist working groups or departments in these domains.

This process complements the one specified in the CLC/TS 50701 [7] by proposing concrete solutions to avoid conflicts among the requirements from the different domains.

Please note that the Policy in this document does not cover the Safety Policy and Security Policy to the maximum extent, but will be included during later phases of the V-cycle, as is in full agreement with EN 50126-1:2017 [1].

Revision history

Version	Change Description	Initial	Date of change
0.00	Initial draft	EZ	26.04.2023
0.01	Consideration of the review comments	EZ, MDV, FN, EDP, AP	03.05.2023
1.00	Final version for R4	JB	26.06.2023

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

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

[3] EN 50128: 2011, "Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems", European Committee for Electrotechnical Standardization (CENELE), June 2011.

[4] EN 50657: 2017, "Railway Applications – Rolling Stock Applications – Software on Board Rolling Stock", European Committee for Electrotechnical Standardization (CENELE), August 2017.

[5] EN 50129: 2018, "Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling", European Committee for Electrotechnical Standardization (CENELE), November 2018.

[6] EN 50159: 2010, "Railway Applications – Communication, Signalling and Processing Systems – Safety-Related Communication in Transmission Systems", European Committee for Electrotechnical Standardization (CENELE), September 2010.

[7] CLC/TS 50701: 2021, "Railway Applications – Cybersecurity", European Committee for Electrotechnical Standardization (CENELE), July 2021.

[8] IEC 61784-3: 2021, "Industrial Communication Network – Profiles – Part 3: Functional Safety Fieldbuses – General Rules and Profile Definitions", International Electrotechnical Commission (IEC), Edition 3, February 2021.

[9] IEC/TS 62443-1-1: 2009, "Industrial Communication Networks – Network and System Security – Part 1-1: Terminology, Concepts and Models", International Electrotechnical Commission (IEC), Edition 1.0, July 2009.

[10] IEC 62443-2-1: 2010, "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 2010.

[11] IEC TR 62443-2-3: 2015, "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.

[12] IEC 62443-2-4: 2017, “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.

[13] IEC/TR 62443-3-1: 2009, “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.

[14] IEC 62443-3-2: 2020, “Security for Industrial Automation and Control Systems – Part 3-2: Security Risk Assessment for System Design”, International Electrotechnical Commission (IEC), Edition 1.0, June 2020.

[15] IEC 62443-3-3: 2013, “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.

[16] IEC 62443-4-1: 2018, “Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirements”, International Electrotechnical Commission (IEC), Edition 1.0, January 2018.

[17] IEC 62443-4-2: 2019, “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.

[18] COMMISSION IMPLEMENTING REGULATION (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009; Official Journal of the European Union, L 121/8-25, 3. May 2013.

[19] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment; Official Journal of the European Union, L 185/6-10, 14. July 2015.

[20] “RAM Strategy within QPRAMSS”, Open CCS Onboard Reference Architecture (OCORA), Doc.-ID: OCORA-TWS07-203, Version: 2.0, Date: 02.12.2022.

[21] “OCORA Quality, Performance, RAM, Safety & Security (QPRAMSS) – Strategy”, Doc.-ID: OCORA-TWS07-201, Version: 1.0, 30.11.2022.

[22] OCORA-TWS07-010 – RAMS – Modular Safety Strategy

[23] OCORA-TWS07-020 – RAMS – Evolution Management

[24] OCORA-TWS07-030 – RAMS – SRAC/AC Management

[25] OCORA-TWS07-100 – CENELEC Phase 1 – Concept

2 Introduction

2.1 Background

Railway applications must simultaneously comply with requirements derived from both functional and non-functional domains such as:

- System functions to provide the operationally required capabilities,
- Reliability, Availability, Maintainability (RAM) to fulfil operational demands,
- Safety functions to protect people from hazards,
- Security functions to protect the railway applications from threats by malicious people,
- Communication functions to establish transfer of data, and
- Human Factors to prevent or lower impact of inappropriate of incorrect use of the railway application.

We have encountered, based on project and operational experience, that potential conflicts may arise between these domains during risk assessment, implementation and demonstration and operation, maintenance and decommissioning-phases, as specified in the V-cycles representation in EN 50126-1:2017 [1].

Some potential conflicts may arise from, but are not limited to:

- component cybersecurity functionalities and the functional architecture,
- the processing time required by security functions and time critical safety activities/functions such as the exchange of emergency messages,
- security functions and usability of the system,
- identified safety and security measures, and
- the continuous assurance of safety and the frequently required updates of security countermeasures, i.e. compatibility issues.

2.2 Purpose

The purpose of this document is threefold. First, it intends to clarify the relationships and potential related issues between functional and non-functional domains a listed in sections 2.1 and 2.3. Secondly, the explanation in this document helps the reader to understand, feel the urgency and help to acknowledge in which phase during the lifecycle of systems these conflicts and challenges may arise. And thirdly, forming the main part of this document, to give clear principles, guidance and direction by providing a Policy for resolving these conflicts.

This document is established by the Technical Work-Stream TWS07 (RAMS) of the Open Control-Command and Signalling (CCS) Onboard Reference Architecture (OCORA), based on the need for having an integral approach covering both RAMS domains and RAMS-related domains in the specification phase of CCS systems. At moment of writing such a policy is not yet available, whilst mandated by the standards (i.e. EN 50126-1:2017 “RAMS Definition” [1] and CLC/TS 50701 “Cybersecurity” [7]).

2.3 Scope

This document and the Policy in particular covers the following functional and non-functional domains, but might be extended in a future release of this Policy:

- System functions,
- Safety functions,
- Security functions,
- Communication functions,
- Reliability, Availability, Maintainability (RAM),
- Human Factors, and
- External influences.

Please note that the Policy in this document does not cover the Safety Policy and Security Policy to the maximum extent, but will be included during later phases of the V-cycle, as is in full agreement with EN 50126-1:2017 [1].

2.4 Applicability

This document and the Policy is applicable to all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major subsystem and to individual combinations of subsystems and components within the major systems, including those containing software. For the context of OCORA, such a system is the Control-Command and Signalling (CCS) system. Please refer to section 4.3.3.1 for a detailed explanation.

The Policy is intended to be used by all stakeholders in charge of the development, integration, maintenance and/or operation of Railway Applications, such as:

- Railway Undertakers,
- Infrastructure Managers,
- Maintainers,
- Original Equipment Manufacturers (OEMs),
- Suppliers or Sub-suppliers of major subsystems, components and/or software, and
- Research & Development or specialist working groups.

2.5 Abbreviations

Abbreviation	Description
CCS	Control-Command and Signalling
CENELEC	European Committee for Electrotechnical Standardization
CM	Common RAMSS Method
CSM	Common Safety Method
EC	European Commission
EN	European Norm
EU	European Union
IACS	Industrial Automation and Control System
IEC	International Electrotechnical Commission
RAM	Reliability, Availability, Maintainability
RAMS	Reliability, Availability, Maintainability and Safety
RAMS+	Reliability, Availability, Maintainability, Safety incl. all other domains such as Communication, Security, Human Factors, and External Influences.
RAMSS	Reliability, Availability, Maintainability, Safety and Security
SecRAC	Security-Related Application Condition
SuC	System under Consideration

Table 1 Abbreviations

2.6 Definition of Terms

Term	Definition
Availability	**Availability** is the ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided (3.6 of EN 50126-1: 2017 [1]).
Human factors	**Human factor** is defined as the impact of human characteristics, expectations and behaviour upon a system. These factors include the anatomical, physiological and psychological aspects of humans. The concepts within human factors are used to enable people to carry out work efficiently and effectively, with due regard for human needs on issues such as health, safety and job satisfaction. The human factor processes have the objective to prevent and reduce systematic design faults. Human factors aim at preventing errors in all phases, not only in the design phase.
Maintainability	**Maintainability** is the ability to be retained in, or restored to, a state to perform as required, under given conditions of use and maintenance (3.37 of EN 50126-1: 2017 [1]).
Quality	**Quality** is the degree to which a set of inherent characteristics, i.e. distinguishing feature, fulfils requirements, i.e. the need or expectation stated, generally implied or obligatory. It ensures the correct development of all domains including their co-system-engineering. Quality processes have the objective to prevent and reduce systematic design faults.
RAM	**RAM** ensures permanent operation including technical and process aspects.
RAMS policy	The **RAMS policy** includes a policy for resolving conflicts between safety and other aspects like availability, reliability, etc. (7.3.2.1e of EN 50126-1: 2017 [1]).
Reliability	**Reliability** is the ability to perform as required, without failure, for a given time interval, under given conditions (3.52 of EN 50126-1: 2017 [1]).
Safety	**Safety** is the freedom from unacceptable risk (3.64 of EN 50126-1: 2017 [1]). Safety protects people from hazards from failures of the SuC.
Security	**Security** is the condition of system resources being free from unauthorised access and from unauthorised or accidental change, destruction or loss (3.1.68 of TS 50701: 2021 [7]). Security protects the SuC from threats from people.
Security policy	**Security policy** contains a set of rules that specify or regulate how a system or organisation provides security services to protect its assets (3.1.75 of TS 50701: 2021 [7]).
SuC functions	**SuC functions** provide the execution of the system functions in operation.

Table 2 Definition of Terms

3 RAMS and RAMS-related Domains

3.1 Inducement

Within the Technical Work-Stream TWS07 (RAMS) of the Open Control-Command and Signalling (CCS) Onboard Reference Architecture (OCORA) initiative, we realised and acknowledged that besides RAMS domains there are other domains which have a relationship with RAM and are potentially conflicting with each other.

To clarify these relationships and potential related issues we have developed a strategy ([20], [21]). This strategy aims to overcome these challenges and give a guidance to the reader. The domains which are included in this strategy includes reliability, availability, maintainability, safety, security, quality, data communication and human factors.

This Policy document builds upon the strategy as defined earlier, however specifically tailored for application at Railway Undertakers, Maintainers, Infrastructure Managers, OEMs, (Sub)Suppliers and specialist working groups or departments in these domains. In this chapter is outlined which domains are relevant, in which way they could potentially conflict, to stress the importance of acknowledging these conflicts, and an introduction is given to the policy to resolve these conflicts.

3.2 RAMS-related domains

When defining a Railway Application (i.e. system for the application in the Railway sector), starting from the basic concept or system definition, it is generally mandatory to follow the RAMS management process as described in the EN 50126-1:2017 [1] standard.

This management process starts with the definition of the “concept” (phase 1) and “system functions” (phase 2) which will be directly related to “system acceptance” (phase 10) and “operation and maintenance” (phase 11) in the V-cycle, by means of validation at a later stage in the system’s life cycle. The standard currently identifies and covers the following ‘classical’ domains:

- Reliability,
- Availability,
- Maintainability, and
- Safety.

Although these domains are at the core of the EN 50126-1:2017 [1] standard, typically for modern Railway Applications in a highly complex environment or as part of a multi-asset system other domains need to be taken into account, which are not (yet) part this this standard. For the ease of convenience, we identify them as ‘RAMS-related domains’, as they have a relationship with RAMS, and might include, but are not limited to:

- Security,
- Quality,
- Data communication, and
- Human Factors.

The majority of these domains have their own standard on how to manage the domain for a specific system or during the life time of a system, e.g. CLC/TS 50701 on “Cybersecurity” [7]. We also recognise a strong relationship with the development phases of the EN 50126-1:2017 [1] standard. This is where the first problem arises. Although both standards stress the importance to encounter the operational context in which the system is or will be used and the need for resolving conflicts

between different domains, they do not provide guidance to identify potential conflicts nor to solve them.

In the following sections these 'challenges' will be elaborated in more detail for a better understanding. Please also refer to the definition of the term and domains in **Table 1** and in section 2.6.

3.3 First challenge: conflicts between RAMS and RAMS-related domains

In addition to the relationships between RAMS and beforementioned RAMS-related domains. The RAMS-related domains could also be interlinked and thus may be in conflict with each other. In this section a number of examples are provided to illustrate these relationships and potential conflicts. In addition to this section, the interlinks between the domains in an operational context is presented in Chapter 6 (Annex 1).

Safety and Security

The domains Safety and Security have a strong relation and might be in conflict because:

- If the system is not secure, it's unlikely to be safe.

Availability and Safety

The domains Availability (of the system or at a higher aggregated level) and Safety have a strong relation since:

- If the system enters a safe state, it's unlikely to be available

For example, a safety target can be achieved by ensuring the system enters a safe state (e.g. all trains stopped) in the event of a particular failure. The defined safe state can depend on operational/maintenance context (e.g. a train at standstill at platform rather than in tunnel). If there are circumstances where this safe state has a significant adverse impact on reliability/availability, then a different and optimised solution might be needed in order to achieve the RAM targets without compromising safety.

Reliability and Security

The domains Reliability and Security have a strong relationship as:

- If the system is not secure, it's unlikely to be reliable (see also example as described above)

Reliability and Human Factors

The domains Reliability and Human Factors (both operational-, maintenance- or passenger related human factor impact) have a strong relationship and might be in conflict because:

- If human factors are not adequately considered, the system is unlikely to be reliable

For example, a reliability target can be achieved by designing the system function in such a way the system could fulfil the requirements. If, however, the system is incorrectly used or maintained (either by unfortunate design provoking misuse or inadequate training) the reliability targets on a higher level (for example train level) cannot be achieved.

Besides Reliability, there is also a relationship with Availability, Maintainability, Safety and Security which is visualised in **Figure 1**.

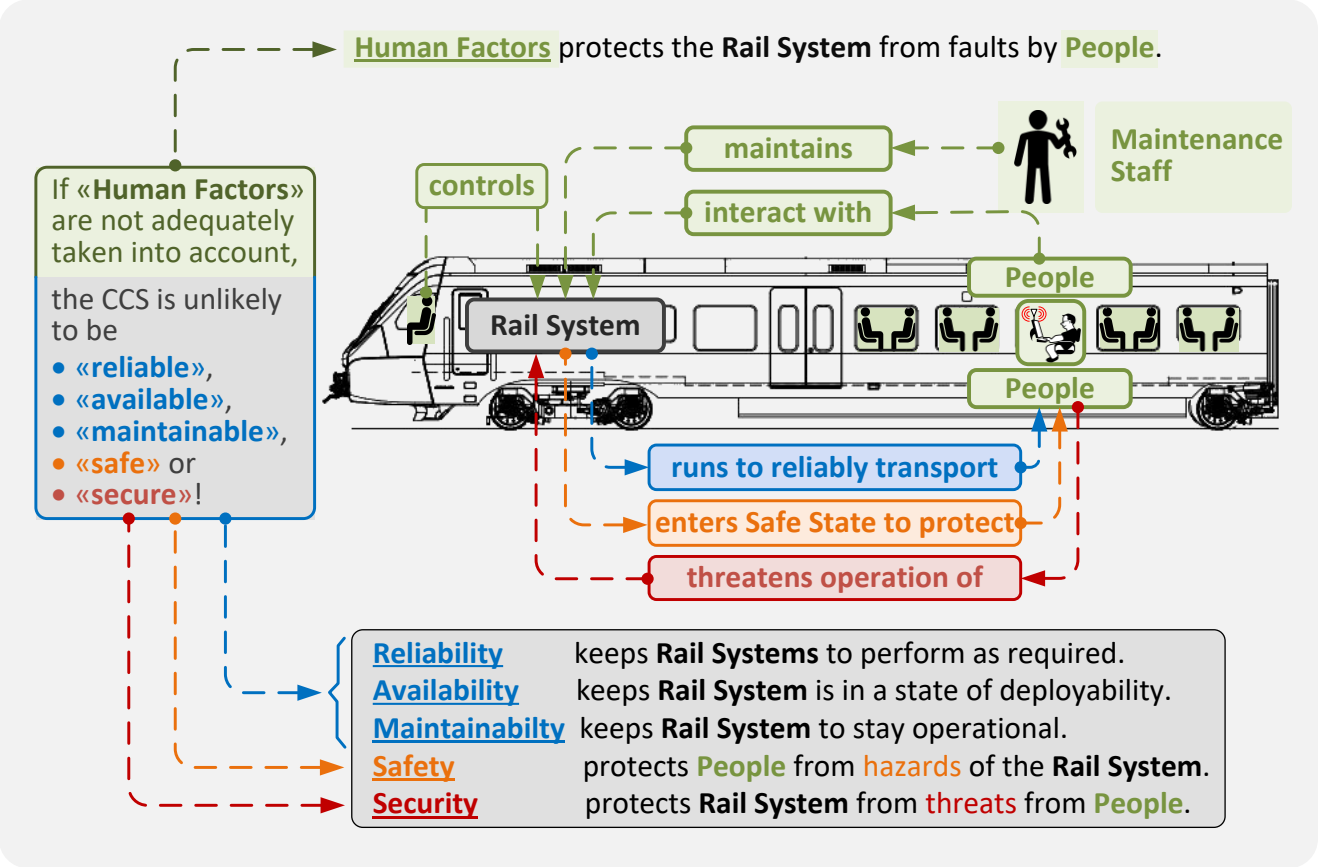

Figure 1 Potential conflicts between the domains human factors and RAM, safety, and security

Besides the (inter)relations and conflicts mentioned in this section, other potential combinations and conflicts (with other domains) can be identified as well. The intention of this section is not be fully complete, but to stress the importance of acknowledging that RAMS and RAMS-related domains generally have strong relationships, they might be in conflict with each other and thus one cannot manage one domain completely separate or independent from the others (i.e. neglecting the effects on other domains).

This challenge will play an important role during the life cycle of a system. One way to cope with this challenge is the introduction and execution of 'co-engineering' in the early phases in the V-cycle, instead of parallel-engineering which is the general practice.

3.4 Second challenge: co-engineering of all RAMS and RAMS-related domains

We have the obligation, but cannot avoid the complexity due, to fulfil the domain-specific requirements simultaneously throughout the phases of the V-cycle of the system. One can imagine, this co-engineering without frequent alignment will lead to difficulties when (design) decisions impacting other domains are neglected or being aligned at a phase in which decisions are irreversible. This forms the second challenge.

For example, in Section 4 of in chapter 7.2 of the EN 50129 [5] standard it is required to include protection against unauthorized access, including physical security threats and IT-security threats. However, when such measures have been implemented it likely has an effect on preventive and corrective maintenance tasks, in terms of accessibility, handling of components and diagnosability,

affecting the throughput time of maintenance. When both domains are not managed integrally, it is likely that maintenance or security targets cannot be fulfilled.

In general, we have identified, by experience, that the lack of alignment between RAMS and RAMS-related domains during development phases in projects could lead to:

- not fulfilling requirements on higher aggregated levels,
- introducing additional costs due to necessary modifications at a later phase, and/or
- not achieving the original project planning due to conflict resolution or accepting concessions on the scope.

This in turn may provoke difficult discussions as:

- the railway operators and infrastructure managers are not keen on accepting compromises on quality, reliability, availability, maintainability and system functions or capabilities,
- the railway safety authorities are not keen on accepting compromises on safety, and
- the railway security authorities are not keen on accepting compromises on security.

This means simultaneous fulfilment of the RAMS and RAMS-related requirements without conflicts is a key success factor for delivering projects within time, costs, scope and quality. This can be seen as the second challenge. To manage these conflicts, section 7.3.2.1e) of the EN 50126-1: 2017 [1] calls for having:

- a (RAMS+) Policy, including principles to solve potential conflicts between RAMS and RAMS-related domains, and
- a (RAMS+) 'mature' Organisation, allocating roles, responsibilities, competences, independences and relationships of organisations to manage, amongst others, potential conflicts between RAMS and RAMS-related domains.

(The term 'mature' is used in this context to describe the level of effort required for co-development, which is typically higher than parallel-development.)

4 RAMS+ Policy

4.1 Inducement

In the former sections the domains of ‘RAMS’ and ‘RAMS-related’ were introduced, alongside with the (inter)relations between them and possible conflicts that may arise during the life cycle of a Railway Application. A key success factor within a project is having a Policy, providing principles to solve potential conflicts between these domains.

The Policy as described in this Chapter is intended to give clear principles, guidance and direction to involve RAMS and RAMS-related domains within the development, integration, maintenance and/or operation phases, i.e. all stages in the V-cycle representation of the EN 50126-1: 2017 [1], and to resolve potential confits.

As the Policy in this Chapter includes all domains as listed in sections 2.1 and 2.3, the term ‘RAMS+ domains’ and ‘RAMS+ Policy’ will be used as indication that besides RAMS, all related domains and interrelations shall be covered.

4.2 RAMS+ principles

At the core of this chapter is the co-engineering of the RAMS+ domains within each phase of the lifecycle model specified

- in the EN 50126-1 [1] for RAMS and
- in the CLC/TS 50701 [7] for cybersecurity.

This co-engineering is challenging because of possible mutual conflicts between the safety and security domain. The following principles, selected in part from Annex D of the CLC/TS 50701 [7], promote the subsequent definition of the RAMS+ policy for resolving conflicts between the RAMS+ domains.

1. The security environment shall protect the essential functions of the system, i.e. the system and the safety functions.
2. Separate security and safety as far as possible but coordinate them efficiently. Hence:
    a. Safety and security targets should not be coupled or integrated because of the many differences between them. However, the processes and lifecycles of these domains need to be coordinated and appropriate interfaces need to be established. In particular, hazards resulting from security problems need to be identified, and they shall be treated as threats in the cybersecurity threat risk assessment. Here the safety engineer needs to provide support in order to assess the safety implications during the cybersecurity assessment, but the derivation of appropriate security countermeasures shall be the responsibility of security engineers in accordance with security standards.
    b. Avoid frequent changes of safety functions.
    c. Ensure that security measures can be easily maintained as security is a collaborative continuous effort and includes human factors as a key element based on
        - system diagnostics,
        - support functions and
        - operational processes.
3. Conflicts between safety and other aspects like availability, reliability, etc. shall be resolved.

4.3 Co-System-Engineering of the RAMS+ domains

4.3.1 Introduction

Firstly, why do we need layered building blocks (functions) of the system? The answer to this question is provided below and results in the need for a system model consisting of layered building blocks (functions).

4.3.2 System model consisting of layered building blocks (functions)

The fulfilment of

- the system functions and
- the safety functions

are ensured by adhering to the development process specified in the EN 50126-1 [1] and EN 50126-2 [2] for the system, and EN 50128 [3] for the software. However, they rely on the functions of several layered building blocks to ensure their proper operation.

A first higher-layered building block is the security functions that protect the system- and safety-functions from attackers such as hackers, criminal organisations or state sponsored groups. These security functions include physical security and IT-security (see section 7.2 of the EN 50129 [5]).

A second higher-layered building block is the communication functions providing the technical means for the reliable, safe, and secure exchange of signals and/or date among the system-, safety-, and security-functions with high availability.

Reliability, Availability and Maintainability (RAM) performances are attributed to each of the four building blocks visualised in **Figure 2** as

1. “core RAM Performance”,
2. “system RAM performance”,
3. “integrated RAM performance”, and
4. “perceived RAM performance” (i.e. from the perspective of passengers, users, etc.).

Note that the Human Factors account for about 70% of the achieved RAM performance of the system, subsystem or component. They are related to, but not limited to,

- inappropriate or incorrect operation, e.g.
    - incorrect man machine interface design,
    - inefficient processes in the transportation chain,
- inefficient or incorrect maintenance, and/or
- vandalism by people.

The control of the human factors is therefore of paramount importance for the achieved RAM performance level of a system – specifically when integrated in the operational context and by the perception of ‘the outside world’ (passengers, public opinion).

Finally, the system, subsystem or component is subjected to a range of “external influences” such as climatic conditions, mechanical conditions, altitudes, and electrical conditions to be maintained within the specified limits to ensure the system’s correct operation.

These layered building blocks (functions) establish the system model depicted in **Figure 2**.

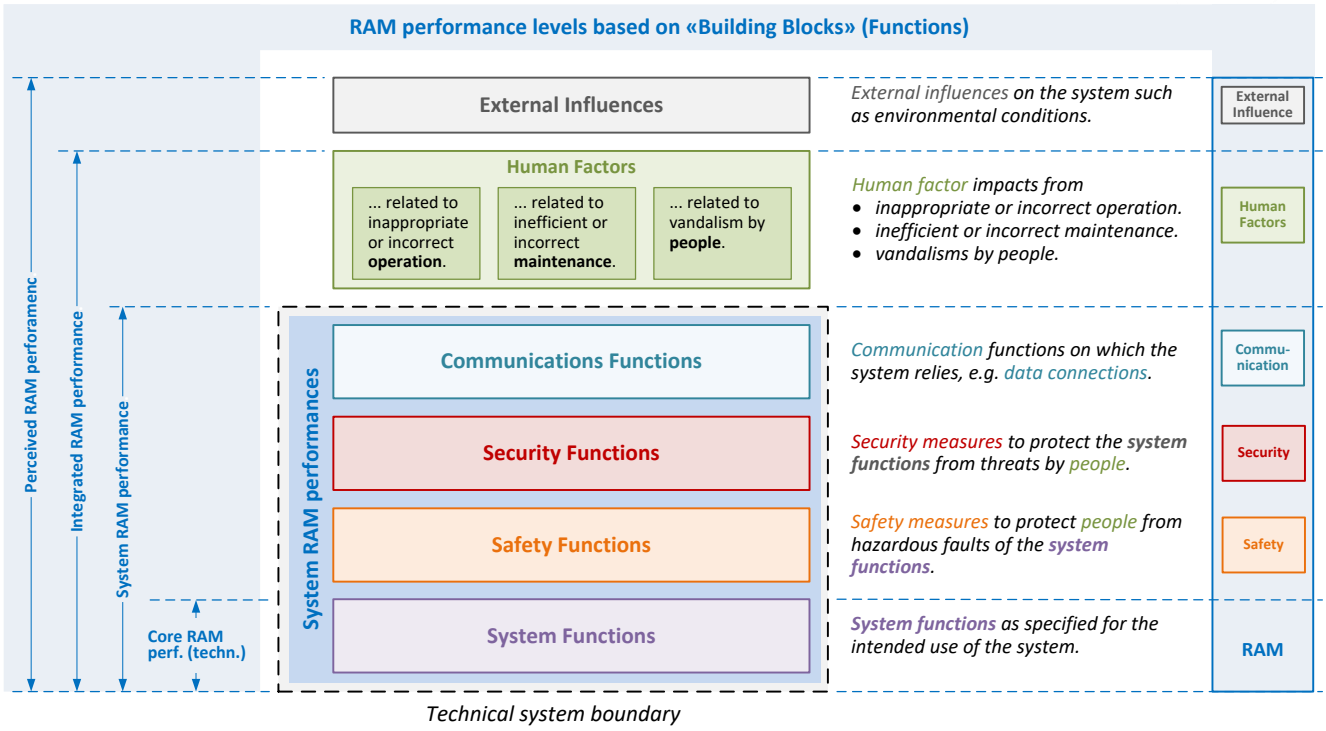

Figure 2 Layered building blocks (functions) of the technical and non-technical parts of the system

4.3.3 RAMS+ Policy

4.3.3.1 Scope

The specification of a railway system, subsystem or component includes domains related to

- system functions,
- safety,
- security,
- communication functions,
- Reliability, Availability, and Maintainability (RAM),
- human factors, and
- external influences.

The requirements of these domains can be interlinked and potentially conflicting with each other. This “RAMS+ Policy” enables to resolve the conflicts among these domains in due consistency with the generic development process described in the EN 50126-1: 2017 [1]. It applies:

- to the specification and demonstrations of RAMS+ for all railway applications and at all levels of such an application, as appropriate, from complete railway systems to major subsystem and to individual combinations of subsystems and components within the major systems, including those containing software, in particular
  - to new systems, subsystems and components,
  - to new systems integrated into existing systems, subsystems and components already accepted, but only to the extent and insofar as the new system with the new functionality is being integrated.
  - to modifications and extensions of existing systems, subsystems and components already accepted. This includes, but not limited to, the extension of legacy systems, subsystems and components with security functions to ensure IT-security.

This RAMS+ Policy contains a set of rules that specify or regulate how a system or organisation:

- deals with and
- enables to resolve

potential conflicts among the RAMS+ domains.

The subsequent rules or regulations ensure the necessary stability and viability of the system-, safety-, and communication-related functions, their documentation, and approvals.

4.3.3.2 Rules or regulations how to deal with potential conflicts

4.3.3.2.1 General rules for dealing with safety and security

This subsection is an excerpt of Annex D entitled “Safety and Security” of the CLC/TS 50701 [7].

1. To ensure the necessary stability and viability of the system-, RAM-, safety-, communication-, and security-related documentation and approvals, it is advisable to separate cybersecurity from these issues adequately to decouple the different lifecycles and the associated approval processes. Otherwise, each change affecting any of these domains may trigger a new approval of the other domains.

   Principle 1*: Safety and security are different and should be treated as such.*

   Principle 2*: Separate security and safety as far as possible but coordinate them efficiently.*

2. Communication and interaction between the teams of the domains shall be implemented throughout the lifecycle and appropriate review processes and intervals shall be maintained.

3. Particularly, the processes of all domains shall inform the other domains about their functions or assets to be protected by the security functions. This information shall be documented ans serves as an input for the cybersecurity risk assessment.

4. The cybersecurity process deals with the risks stemming from attacks and malicious interventions, implementing cybersecurity requirements in the system, subsystem or component or exporting some security-related application conditions (SecRAC).

   If cybersecurity threats have potential impacts on the system-, safety- or communication-functions of the system, the cybersecurity case shall include or refer evidence on how security threats with the potential to affect these functions have been evaluated and how protection against the adverse influence has been achieved.

5. Application of a security patch impacting safety functions shall be coordinated with safety management.

6. The cybersecurity case and its SecRACs shall be communicated to the system-, safety- and communication-related management. If any of these managements considers SecRACs to potentially impact their functions, they shall then be considered as requirements to be fulfilled by the building block(s) above it.

   Principle 3*: The security environment should protect essential functions, incl. safety.*

7. Security Levels (SL) according to IEC 62443 ([9] - [17]) are defined with respect to the type of attacker. SL 1 represents unintentional errors or foreseeable misuse only, while SL 2, SL 3 and SL 4 relate to intentional attacks in which the attacker possesses increasing levels of knowledge, motivation and resources. As safety considers security as an environmental condition it is immediately evident that measures according to any particular SIL do not cover measures against intentional attacks. However, errors and foreseeable misuse also need to be addressed by safety systems, so any safety system should also cover SL 1, at least for requirements related to integrity. But for other SLs there is no automatic correspondence between SL and SIL as the SL will always depend on the security environment. And it should

also be noted that security requirements cannot be fulfilled only by IT measures, but physical security measures are also necessary. In summary the following principle is established

***Principle 4**: Safety and Security Target measures should not be coupled.*

8. The fulfilment of the high-level cybersecurity objectives is demonstrated as part of the cybersecurity case. Either they are fulfilled by the cybersecurity functions or under certain security conditions and assumptions (SecRAC).

   Note that no single security measure should be regarded as sufficient. There should always be a second line of defence which protects against an attack. This concept is called “defence in depth”. It does not mean that the security measures need to have the same effectiveness, but even for the most effective security measure there should be a fall-back. This implies that security measures should also be monitored for their effectiveness.

9. Because of the many differences it is not reasonable to integrate safety and security. However, the processes and lifecycles need to be coordinated and appropriate interfaces need to be established.

   In particular, in safety risk analysis, hazards resulting from security problems need to be identified, and they are then treated as threats in the cybersecurity threat risk assessment. Here the safety engineer needs to provide support in order to assess the safety implications during the cybersecurity assessment, but the derivation of appropriate security countermeasures is the responsibility of security engineers in accordance with security standards.

   ***Principle 5**: Cybersecurity threats and risk analysis is the main interface with the safety analysis.*

10. The cybersecurity case shall be maintained and updated regularly. If the cybersecurity functions are changed, it has to be demonstrated that the safety-related cybersecurity objectives still hold (including the exported SecRAC). If necessary, the cybersecurity case can be assessed and certified according to the relevant cybersecurity standards.

    The provision of security is a joint effort of the operators (often called asset owners in security), the system integrators (who supply complete systems) and the suppliers (who sell components). But unlike safety, the evaluation processes operate at a higher frequency in security. Even without any incident it is good practice to update threat risk assessments at least once per year and to feed the results forward and backward to the stakeholders at the interfaces. So, the conclusion is

    ***Principle 6**: Security is a collaborative continuous effort.*

As a result of this documentation structure, the documentation regarding functional safety can be considered stable and viable so long as the cybersecurity process is properly adapted to changing threat scenarios. Hence, while the security documentation may be subject to frequent updates as a result of the volatile threat landscape, the safety approval can remain valid.

4.3.3.2.2 Specific rules enabling to resolve potential conflicts among the RAMS+ domains

The presence of conflict among requirements of the different domains is not always apparent. Nor is there a generally known and accepted method that ensures their complete detection.

Rule

*Requirements on any level of the hierarchical building blocks (functions) that might be impacted by the specification, performance or characteristic of any overlaying building block shall be exported to any of the overlaying building blocks visualised in **Figure 3**.*

Example 1

The safety- and security-functions require that the communication functions use appropriate protocols that ensure the required level of safety- and security-level.

Example 2

The proper operation of the system-, safety-, and security-functions, adherence to the specified transmission and response times of data packages must be ensured. Deviations from these timing requirements must be detected and appropriate reactions of the system, subsystem or component must be implemented.

The rule stated above ensures the necessary stability and viability of

- the system-, safety-, security- and communication-related functions on the system-, subsystem- and component-level,
- their documentation, and
- their approvals.

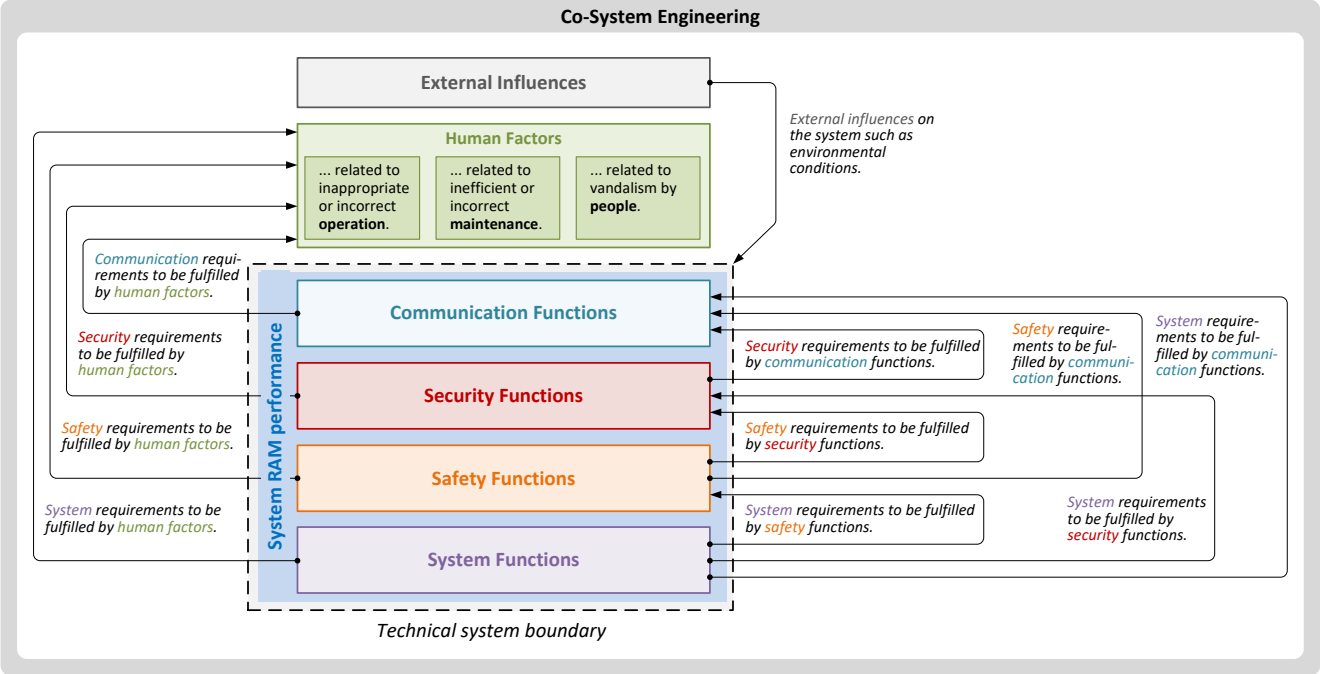

Figure 3 RAMS+ policy – the resolution of potential conflicts among the RAMS+ domains

4.3.3.2.3 Possible implementations

One possible solution to achieve the necessary levels of separation and coordination between cybersecurity and safety processes is to define only a limited number of coordinated cybersecurity objectives on a high level. These objectives need to be fulfilled through security requirements or security-related application conditions.

Example 1

For safety-critical communication, the high-level cybersecurity objective could be “The safety-critical messages has to be protected against manipulation”.

Example 2

The high-level cybersecurity objectives can also be related to a safety-critical item list. In this case, the high-level cybersecurity objective could be “The functions of the safety-critical items has to be protected against manipulation.”

5 Recommendations

The RAMS+ Policy in this document, as outlined in Chapter 4, suggests an extension of:

- the generic RAMS engineering process specified in the EN 50126-1: 2017 [1] and EN 50126-2: 2017 [2].
- the software engineering process specified
  - in the EN 50128: 2011 [3] for programmable electronic systems for use in railway control and protection applications and
  - in the EN 50657: 2017 [4] for programmable electronic systems for use in rolling stock applications.
- the provision of safe and secure communication as specified in the EN 50159: 2010 [6], IEC 61784-3: 2021 [8], CLC/TS 50701: 2021 [7] and the series IEC 62443 [9] - [17].
- the approval of the functional and technical safety and security of the SuC as specified in the EN 50129: 2018 [5].

6 Annex 1: Visualization of mutual interrelations

The states and the change of the domain

- availability,
- maintenance,
- system, subsystem, or component,
- safety, and
- security

affects the other domains as they are mutually interlinked. These states depend on event such as

- failures of external systems,
- failures of the system function(s),
- failures in the defence of security attacks, and
- human errors.

This is visualised in **Figure 4**. The simultaneous fulfilment of all requirements requires therefore a co-system-engineering of all domains within all phases of the life cycle of the system, subsystem or component.

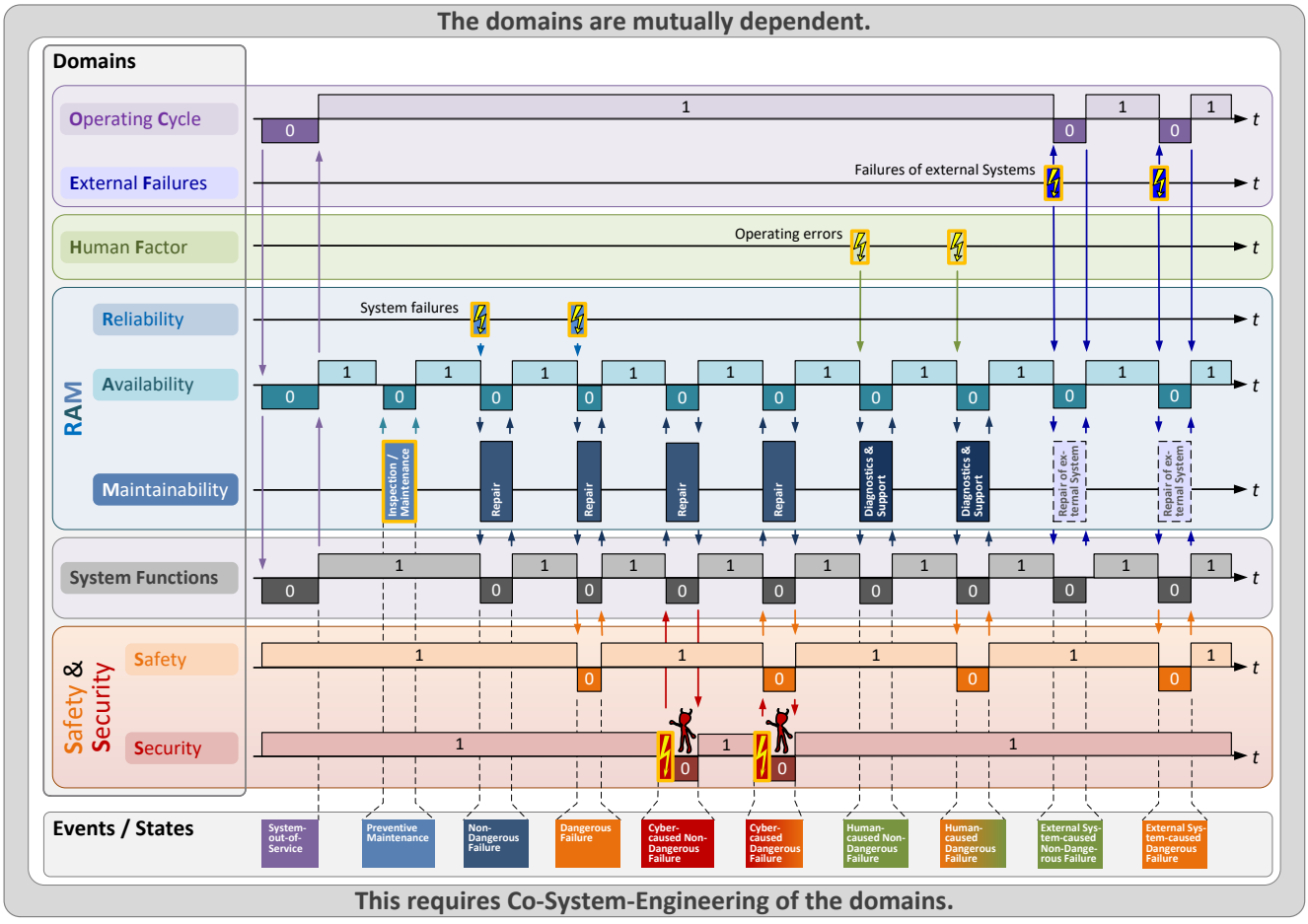

Figure 4 Mutually dependence of the RAMS+ domains