OCORA

Open CCS On-board Reference Architecture

RAM Strategy within QPRAMSS

Document ID: OCORA-TWS07-050

Version: 2.00

Date: 02.12.2022

Management Summary

This RAM Strategy has especially been created for highlighting the complexity to manage Quality, Performance (i.e. System Capabilities), Reliability, Availability and Maintainability (RAM), Safety, and Security (QPRAMSS) in the design of CCS. Today, the QPRAMSS domains are managed separately because of the lack of an overarching approach. This will undoubtedly lead to huge risks affecting the time and costs of CCS development projects and it is specifically applicable to OCORA.

With this RAM Strategy we took the opportunity to propose a solution to cope with the separation of the QPRAMSS domains knowing that this should be covered on an overarching OCORA QPRAMSS Strategy level.

This RAM Strategy therefore outlines the required interaction between the different TWSs and BWSs to align deliverables of each phase to avoid conflicting requirements. This prevents that potentially unacceptable large compromises have to be made in the functional architectural design or in QPRAMSS requirements towards the end of the project (phase 4 out of 5). Secondly, the RAM Strategy defines the objectives and the approach; however, the specific activities, and deliverables of each phase will be described in the RAM Plan (part of the QRAMSS plan).

The proposed approach of synchronisation between QPRAMSS aspects and domains has been included in chapter 3. This shall ensure and improve collaboration between all Technical Work-Streams (TWSs) and Business Workstreams (BWSs) in charge of developing the new CCS and shall also be used withing the PRAMSS Europe's Rail Joint Undertaking (ERJU) System Pillar domain. This approach is also required by the recent CENELEC Technical Specification TS 50701 [13].

Revision history

Version	Change Description	Initial	Date of change
0.01	Draft for Release R2. Document ready for review.	EZ	17.05.2022
0.02	Consideration of the review comments	AP	08.06.2022
1.00	Official release for R2	JB	09.06.2022
1.01	Document redrafted.	EZ	02.09.2022
1.02	Document updated according to review comments.	EZ	06.09.2022
1.03	Document updated according to Workshop in Berlin	EZ	27.10.2022
1.04	Consideration of the review comments. Formal updates	AP	02.11.2022
1.05	Consideration of the review comments.	AP	22.11.2022
2.00	Official release for R3	AP	02.12.2022

Table of Contents

Table of figures

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references 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] EN 50126-1: 2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, CENELEC, Oct. 2017

[8] EN 50126-2: 2017 – Railway Applications – Specification and Demonstration of Reliability, Availability, Maintainability ans Safety (RAMS) – Part 2: System Approach to Safety, CENELEC, Oct. 2017.

[9] EN 50128: 2011 – Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems, CENELEC, June 2011.

[10] EN 50657: 2017 – Railway Applications – Rolling Stock Applications – Software on Board Rolling Stock, CENELEC, August 2017.

[11] EN 50129: 2018 – Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling, CENELEC, Nov. 2018.

[12] EN 50159: 2010 – Railway Applications – Communication, Signalling and Processing Systems – Safety-Related Communication in Transmission Systems, CENELEC, Sept. 2010.

[13] TS 50701: 2022-01 – Railway Applications – Cybersecurity, CENELEC, Jan. 2022.

[14] 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.

[15] 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, Nov. 2010.

[16] 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.

[17] 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, Aug. 2017.

[18] 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.

[19] 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.

[20] IEC 62443-3-2: 2013 – Industrial Communication Networks – Network and System Security – Part 3-3: System Security Requirements and Security Levels, International Electrotechnical Commission (IEC), Edition 1.0, Aug. 2013.

[21] 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, Jan. 2018.

[22] 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), Feb. 2019.

[23] OCORA-TWS01-030-System-Architecture

1 Introduction

1.1 Purpose of the document

This document – the “OCORA RAM Strategy” - defines the procedure to specify the RAM targets of the OCORA CCS and its subsystems for

- Phase 0 “Prerequisites” of the TS 50701 [13],
- Phase 1 “Concept”,
- Phase 2 “System Definition and Operational Context”,
- Phase 3 “Risk Analysis and Evaluation”,
- Phase 4 “Specification of System Requirements”, and
- Phase 5 “Architecture and apportionment of system requirements” of the EN 50126-1 [7].

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 or within PRAMSS domain of the ERJU System Pillar, information provided in this document can be used as input for your development.

1.2 Applicability of the document

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

1.3 Context of the document

This document is published as part of the OCORA R3, 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].

The Whitepaper on RAM Strategy is connected to other RAMS deliveries, like this document, which are also part of the R3 release. The Figure 1 presents the link between the different deliverables. It must be noticed that the Whitepapers on SRAC/AC Management, on Evolution Management, on Optimized Approval Process and on RAM Strategy are additional documents besides the documents according to the formal CENELEC V cycle Documentation (represented in black in the figure below) required for the new modular approach.

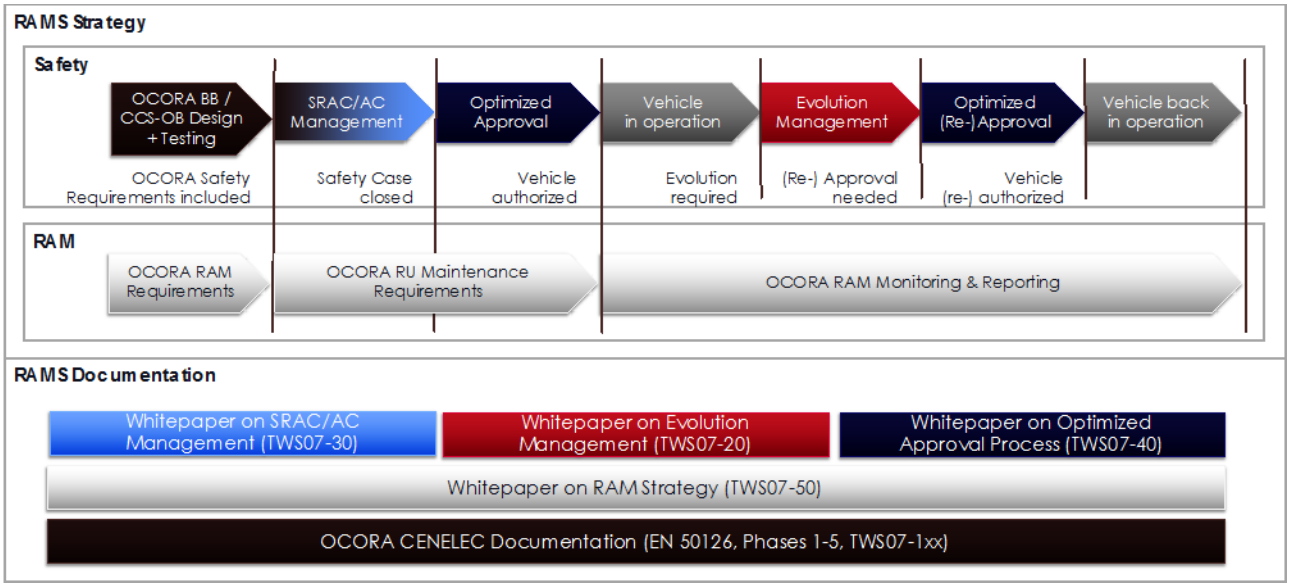

Figure 1 OCORA RAMS Strategy and RAMS Documentation

2 Overview of the OCORA RAM strategy

2.1 Introduction

The purpose of OCORA is to specify the “Open Control-Command and Signalling (CCS) Onboard Reference Architecture” with the goal of enabling the successful integration of all required subsystems/components from different vendors into a

1. reliable,
2. safe,
3. cybersecure,
4. fully functional, and
5. approvable

open onboard CCS.

This document – the “OCORA RAM Strategy” – does not defines the procedure to specify the RAM targets of the OCORA CCS and its subsystems. This will be covered by the RAM Plan (part of the QRAMSS plan to be released in the future of OCORA). It aims at creating the prerequisites for the preparation of the RAM Plan (part of the QRAMSS plan to be released in the future of OCORA).

This is required at resolving conflicts between RAM and other aspects of the CCS such as safety and (cyber) security (see section 7.3.2.1 in EN 50126-1: 2017 [7]) considering the synchronization points introduced in section 5.1, 5.2, 5.3, 5.5.5, Table 1 and Fig. 6 of TS 50701 [13]. For this purpose, interrelations with the other TWSs are mandatory as described in chapter 3.

2.2 Core of the RAM strategy

The RAM strategy within OCORA is about developing effective RAM requirements for the technical reliability, maintainability, operations and maintenance of the future Open Onboard CCS that suits most of the operational conditions in Europe. In the development process of RAM specifications, the operational conditions, maintenance practices and reliability data of existing ETCSs of the European railway operators will be collected, compared and assessed to reflect a standard set of suitable parameters and their values. Based on this assessment, a derived set of technical and process requirements will be extracted, which will be suitable and feasible for most of the operators.

It must be stressed that the achievable Availability is the result of two elements:

- “Reliability and Maintainability” (technical and process specifications) and
- “Operation and Maintenance” (process of specifying human factors in the design to ensure a robust implementation)

as depicted in Figure 2.

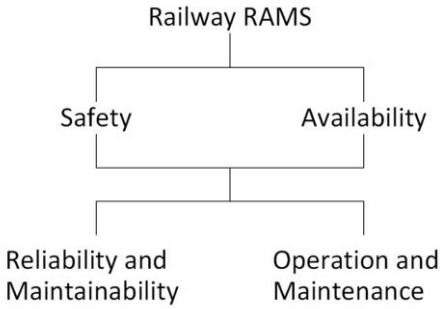

Figure 2 Interrelation of railway RAM elements (from EN 50126-1 [7]). Please note that the word “maintainance” appearing in Figure 2 of the EN 50126-1 [7] has been changed for “maintenance”.

Secondly, because we are co-developing the RAM requirements alongside the other Technical Workstreams (TWS) which focus on e.g. the System Capabilities, Communication, Safety (mentioned in Figure 2) and Security, it is compulsory to align the results of each development phase with the other TWSs to avoid conflicting requirements. It is therefore of utmost importance that the required interrelations between the OCORA Technical Workstreams (TWSs) are well organized. The strategy to achieve this indispensable goal is described in detail in Chapter 3.

2.3 Scope of the RAM strategy

The scope of this "OCORA RAM Strategy" is restricted to:

- Phase 0 "Prerequisites" of TS 50701 [13]

including the first five

(5) phases specified in the EN 50126-1 [7], i.e.

- Phase 1 "Concept",
- Phase 2 "System Definition and Operational Context",
- Phase 3 "Risk Analysis and Evaluation",
- Phase 4 "Specification of System Requirements", and
- Phase5 "Architecture and apportionment of system requirements.
-

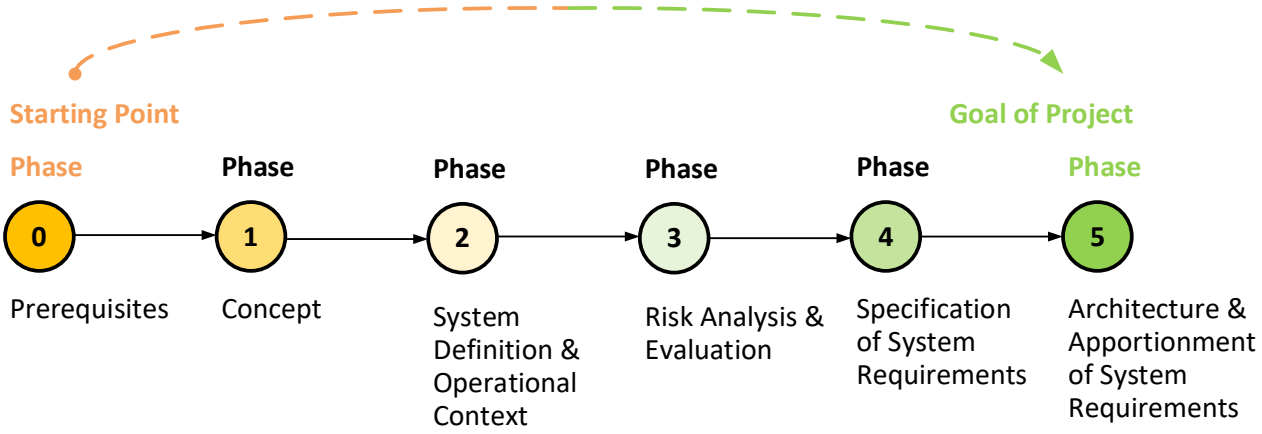

Figure 3 Scope of the RAM strategy covering Phase 0 from the TS 50701 [13] and Phase 1 until Phase 5 from EN 50126-1 [7]

The actual content of each of the five (5) phases will be covered in the RAM Plan (part of the QRAMSS plan) following this RAM-Strategy.

3 Synchronisation points among QPRAMSS aspects and domains

3.1 Introduction

The development of the OCORA Onboard CCS within the different TWSs will create conflicting requirements at least between RAM, Safety, and Security that need to be avoided.

Hence, the synchronisation of the work performed by the different TWSs is strongly recommended in this chapter and impacts the content of the RAM Plan (part of the QRAMSS plan). Please be aware that these synchronisation activities must be included in the plans of the other TWSs.

Note

1. This chapter will be addressed in the Quality, Performance (i.e. System Capabilities), Reliability, Availability, Maintainability, Safety, and Security (QPRAMSS)-Plan. However, the content is also kept in the RAM-Strategy (this document).
2. A key objective of this chapter is to ensure and improve collaboration between all TWSs and BWSs developing a QPRAMSS CCS by proposing a suitable approach and to provide support in implementing this approach.

3.2 RAM, Safety, and Security are closely intertwined

3.2.1 Overview

The design of the Open CCS Onboard Reference Architecture (OCORA) requires, as illustrated in Figure 4, the specification of requirements regarding:

1. System Capabilities,
2. RAM, especially regarding availability,
3. Safety and the provision of full evidence thereof in the safety case to ensure approval by the authority,
4. Security with verifiable proof of complete defences in depth against all possible threats.

These five aspects of requirements are potentially conflicting, as:

- a system that is not secure is unlikely to be safe,
- a system that is safe is likely to be less available,
- a system that is not reliable is unlikely to be neither safe nor secure, and
- a system that does not take human factors into account is likely to be less available, less safe, and less secure
- a system that does not ensure the correct development of all aspects including the synchronisation points, it likely not to be free of conflicts between Performance, RAM, Safety, Security, and Human Factors.

Therefore, a QPRAMSS policy shall be established which shall include a policy for resolving conflicts between safety and other aspects such as System Capabilities, availability, reliability or security.

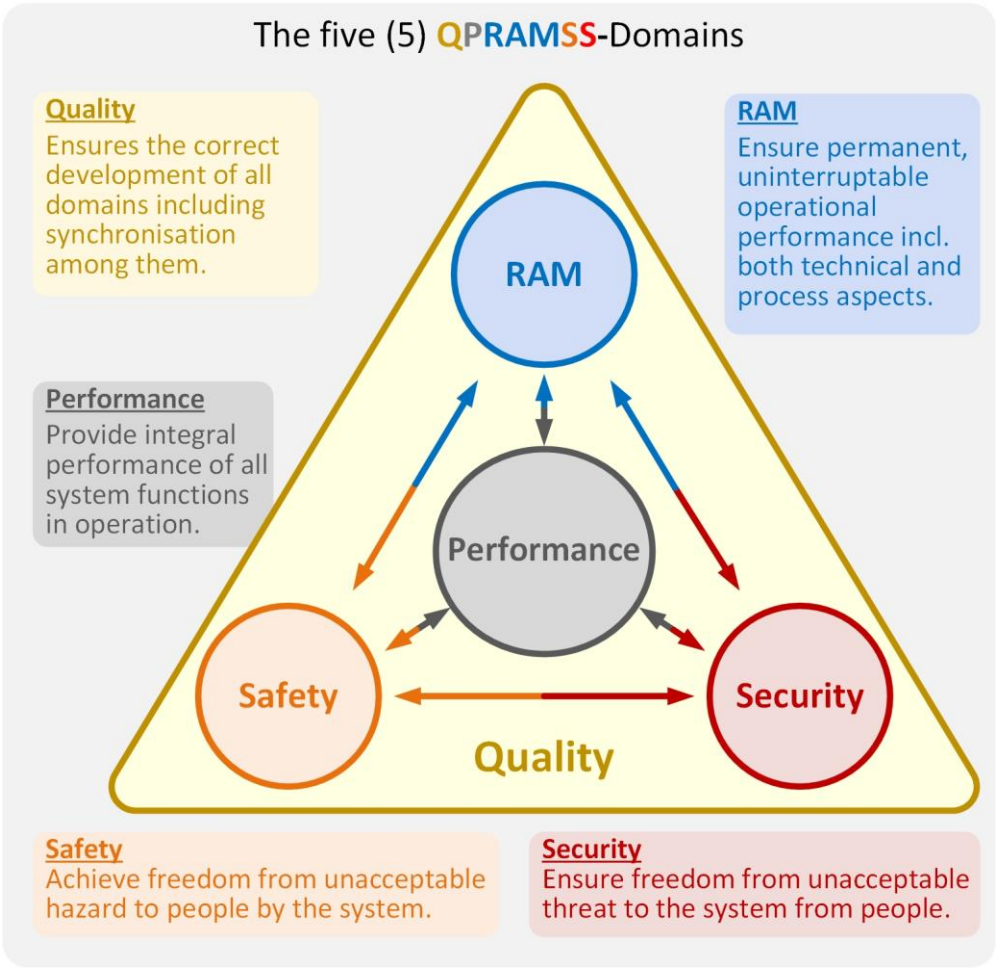

Figure 4 The five domains of requirements to be met simultaneously

3.2.2 Security vs. Safety

Figure 5 illustrates conflicting requirements among Safety and Security. Safety protects people from hazards of the rail system. Security protects the system from threats by people. The two aspects, Safety and Security, are mutually dependent and therefore require mutual coordination in order to fulfil the required level of safety and cyber security. Additionally note that

If the CCS is not "secure", it is unlikely to be "safe"!

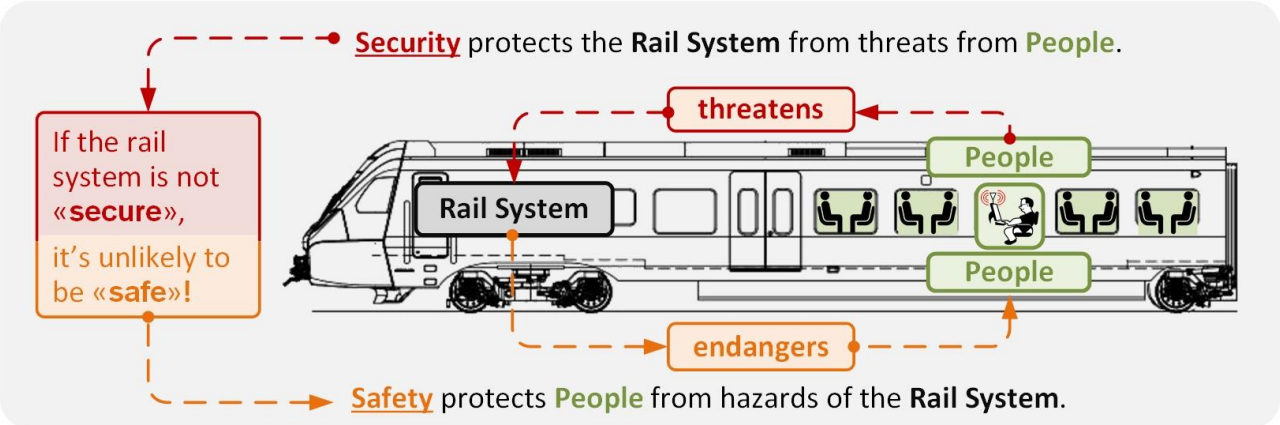

Figure 5 Conflicting aspects to ensure both Safety and Security

3.2.3 Safety vs. Availability

The same applies for the RAM and the Safety of a system as the RAMS elements are interlinked in the sense that a weakness in any of them or mismanagement of conflicts between their requirements can prevent achievement of a dependable system. 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 is needed in order to achieve the RAM targets without compromising safety. With reference to Figure 6 and Figure 7, note:

If the CCS is not "safe", it is not fully "available"!

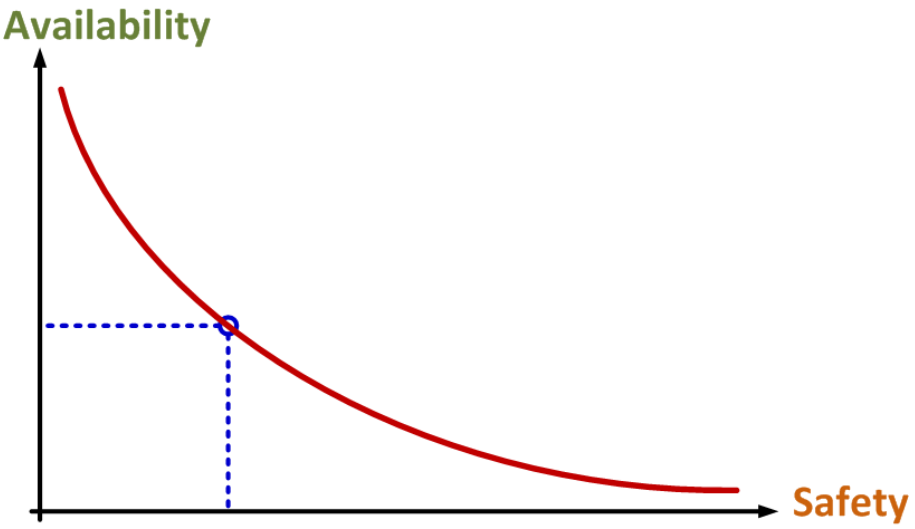

Figure 6 Conflicts arising between Availability and Safety (see 7.3.2.1 in the EN 50126-1 [7])

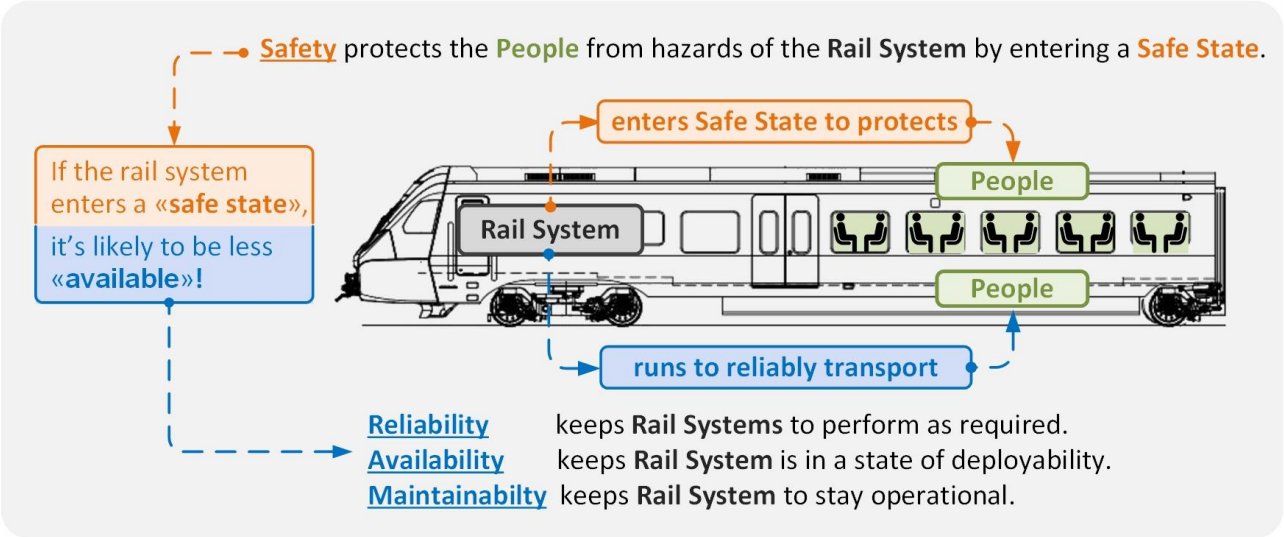

Figure 7 Conflicting aspects to ensure both RAM and Safety

3.2.4 Security vs. Availability

Additionally, RAM requirements might conflict with security measures such as regarding the system integrator and the asset owner illustrated in

Figure 8. Hence,

If the CCS is not "secure", it is unlikely to be "available"!

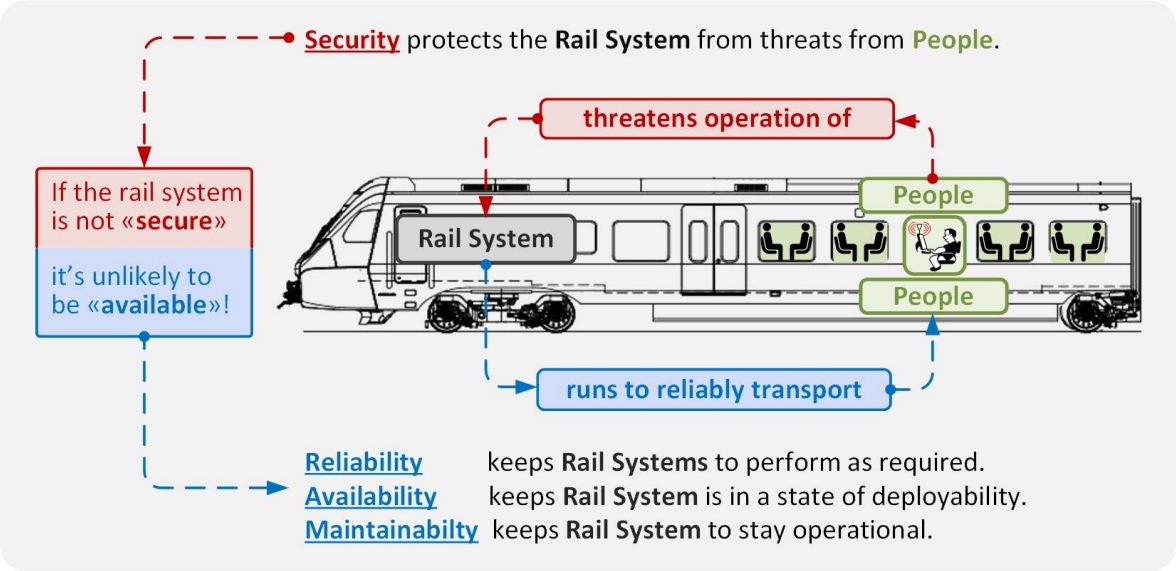

Figure 8 Conflicting aspects to ensure both Security and RAM

3.2.5 Human Factors Matters

Finally, Human Factor requirements might conflict with all other aspects, i.e., RAM, Safety, and Security as illustrated in Figure 9: This is due to the fact that Human Factors relate to faults by

- the driver,
- the passengers including people that are not onbooard the train, and
- the maintenance staff.

Hence,

If the CCS does not take Human Factors into account, it is likely to be less available, less safe, and less secure!

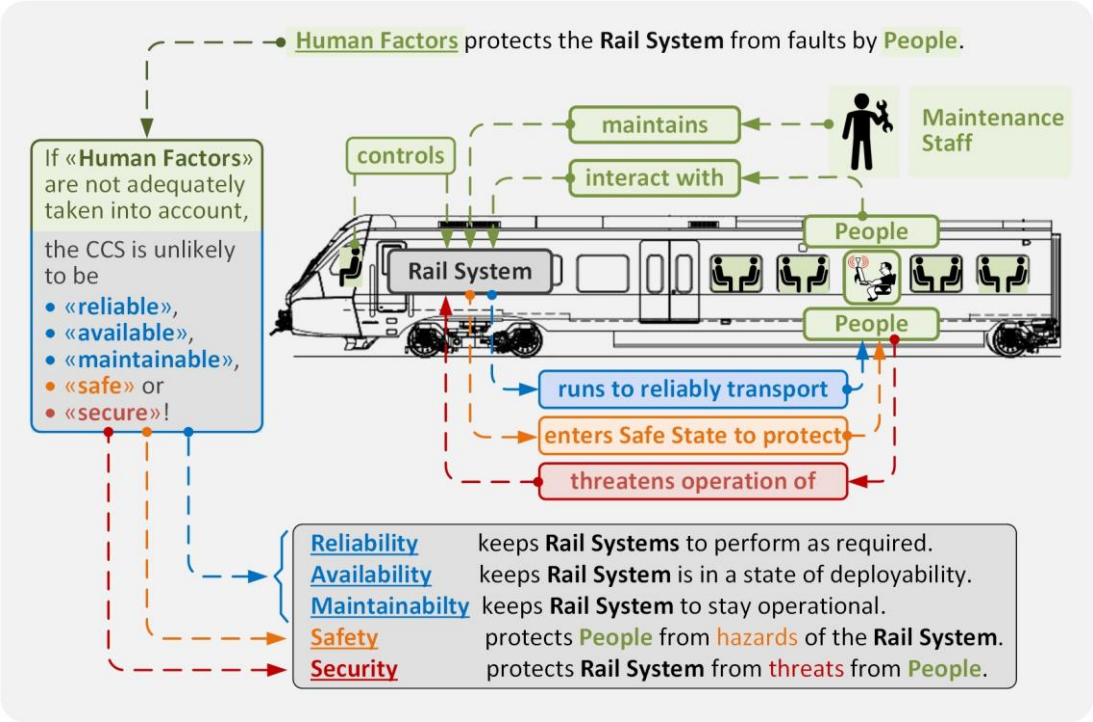

Figure 9 Conflicting aspects to ensure Human Factors, RAM, Safety, and Security. People who threaten the train must not be necessary onboard.

3.2.6 Synchronisation of all five aspects is paramount

This calls for synchronisation of the RAM lifecycle phases specified in the EN 50126-1 [7] with the corresponding security-related deliverables specified in the TS 50701 [13]. The new Technical Specification TS 50701: 2022 [13] published by CENELEC has this necessity as its core.

To ensure the legally required, approval-relevant personal safety, compliance with all safety requirements of the well-known railway standards EN 50126-1 [7], EN 50126-2 [8], EN 50128 [9], EN 50657 [10], EN 50129 [11] and EN 50159 [12] is mandatory. It is important to note that:

> **the safety integrity thus achieved and its demonstration in the safety case loses its credibility to the extent that the fulfilment of corresponding cyber security requirements is not fully verifiable.**

Therefore, the RAM and Safety requirements must be specified together with the security requirements along the development process detailed in the CENELEC Technical Specification TS 50701 [13] and the IEC 62443 series [14] - [22] of international standards. This is the core of the new TS 50701 [13] and this is important to be duly observed since the requirements specifying System Capabilities, RAM, Safety and Security requirements are closely interconnected!

The core challenge of simultaneously fulfilling all QPRAMSS requirements is

- to ensure completeness,
- to manage the complexity,
- to guarantee the complete verifiability, and
- to achieve an optimal balance among the five aspects, i.e. QPRAMSS.

3.3 Reliable & available communication matters

The fact that System Capabilities, RAM, Safety and Security are interconnected has consequences for communication links within the CCS as well as externally. As illustrated in Figure 10, reliable communication is a prerequisite for the provision of safe and secure communication. Communication must be uninterruptible by intentional and unintentional interference to ensure its permanent

availability. Hence, RAM requirements are at the core of all communication links.

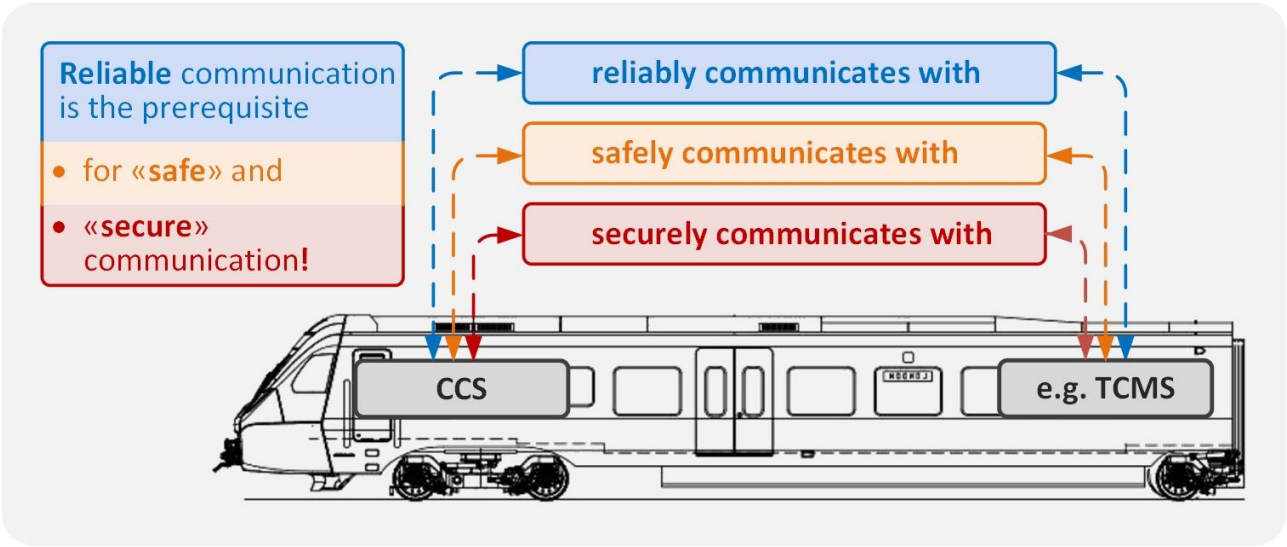

Figure 10 Reliable communication is a prerequisite for safe and secure communication

Figure 11 shows exemplarily a block diagram of a communication system that ensures simultaneously

- RAM, especially availability,
- Safety, and
- Security

of the exchanged data packages. To ensure a communication link that is

- Available, the modulation / demodulation must provide immunity against intentional and unintentional interference.
- Reliable, data corruption must be prevented by channel coding techniques allowing both, the detection and correction of incorrect data.
- Safety, safety approved protocols in compliance with the EN 50159 [12] shall be implemented.
- Security, unsecure data shall be detected and rejected using security- and cryptographic-techniques specified in the TS 50701 [13] and the IEC 62443 series [14] - [22] of international standards.

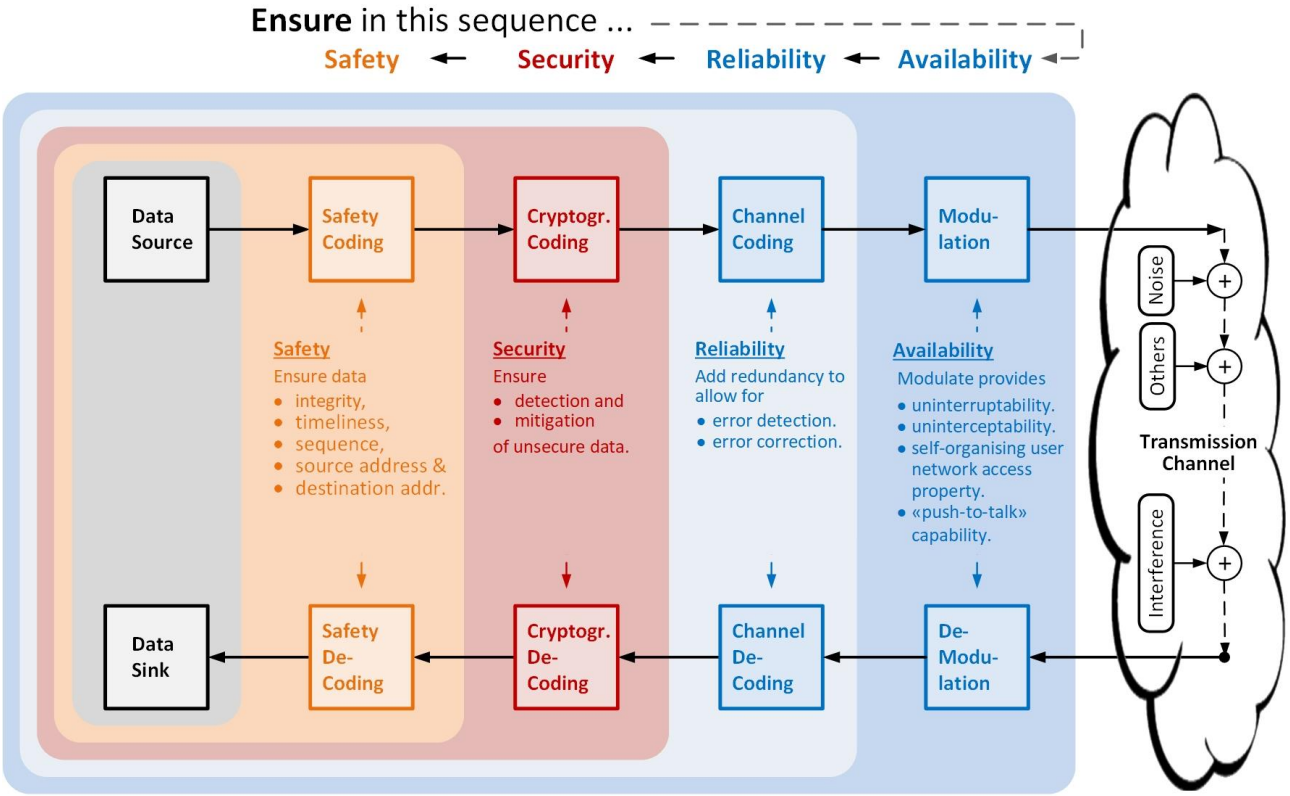

Figure 11 Block diagram of a reliable, available, safe & secure radio and non-radio communication system

3.4 Synchronisation points among all aspects

To prevent conflicting requirements between aspects such as Performance, RAM including Human Factors, Safety, and Security, synchronization points as mandated in the TS 50701 [13] are of utmost importance within each development phase.

This, however, requires that all stakeholders follow in a coordinated way the development of the new Open Onboard CCS in accordance with the development process and its sequence of phases specified in the TS 50701 [13], EN 50126-1 [7], EN 50128 [9], and EN 50657 [10], i.e. that

- the Technical Work Streams (TWS)
  - TWS01 “System Architecture”,
  - TWS02 “CCS Communication Network”,
  - TWS03 “Computing Platform”,
  - TWS04 “Functional Vehicle Adaptor”,
  - TWS05 “Requirements”,
  - TWS06 “(Cyber) Security,
  - TWS07 “RAMS”,
  - TWS08 “Monitoring, Diagnostics, Configuration and Maintenance”,
  - TWS09 “Testing”, and
- the Business Work Streams (BWS)
  - BWS02 “Communication”,
  - BWS08 “Methodology & Tooling”, and
  - BWS09 “Acceptance of Global Standards”

to adhere in a coordinated way to the development phases and mutually exchange all relevant information with the aim of identifying and resolving conflicting requirements in time.

To this end, the activities to be performed by each stakeholder at these synchronization points, illustrated in Figure 12 ,include, but are not limited to

- the mutual exchange of deliverables,
- the review of the deliverables regarding impacts on each stakeholder’s work products at the end of each phase,
- the mutual communication of these impacts and conflicts among all stakeholders, and
- the resolution of these impacts and conflicts in such a way that each stakeholder achieves its objectives!

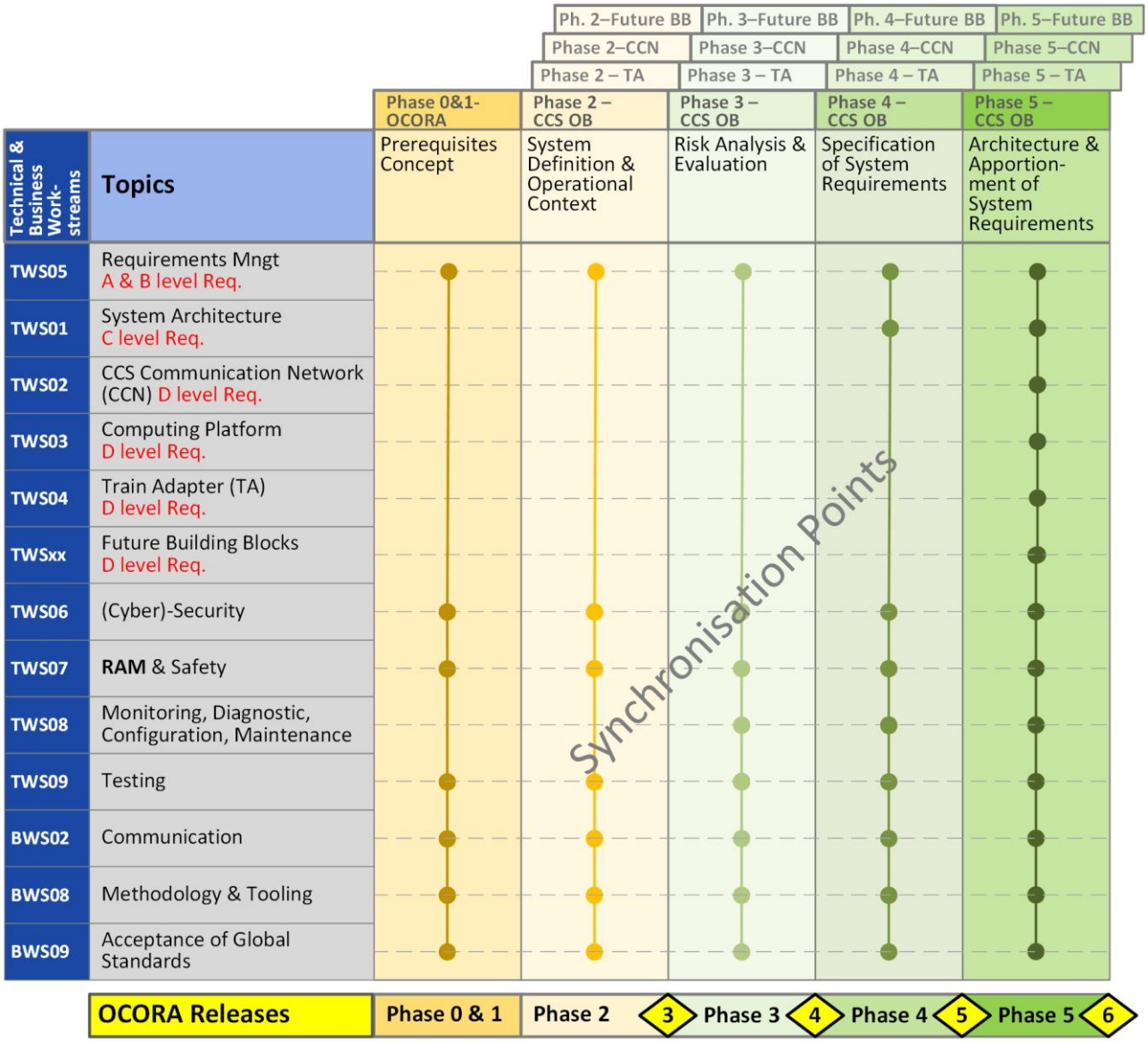

Figure 12 Synchronization points in accordance with the TS 50701 [13] with indication of the corresponding OCORA Releases.

Note that the resolution of these conflicts should be based on a good balance and/or equivalent alternatives

- to mitigate the risk associated with hazards through safety measures and functions,
- to defend against threats through security measures and functions,
- to assure reliability, availability and maintainability through reliability and maintenance engineering, and
- to prevent human errors through adequate design, training, documentation, and on-site support

for the Open CCS Onboard Reference Architecture.

3.5 Quality Management of PRAMSS

The enforcement of a coordinated approach of the numerous TWS and BWS along the phase-oriented V-model with the synchronisation points among the TWS and BWS is indisputably a very challenging task to be performed. It involves

- the review of all deliverables of each TWS and each BWS at the end of each phase and
- the resolution of all conflicting specifications without compromises regarding the required level of availability, safety, and security.

Because of this, there are risks that

- a lot of documents dealing with different aspects have to be reviewed – at least in phase 5 – by people of other TWSs and BWSs who might not have the specific experience and/or knowledge to detect possible conflicting requirements or objectives.
- if conflicts have been detected, no consensus can be found without large compromises.
- proactive activities within TWS01 “System Architecture” as of phase 4 will potentially lead to unacceptable large compromises which might have to be made in the functional architectural design or QPRAMSS requirements.

As a solution, it is here proposed

1. to divide each phase into subsequent four sub-phases dedicated to Performance, RAM, Safety and Security in order to be fully synchronised as shown in Figure 13. Each sub-phase must be completed and approved before moving to the next sub-phase.
2. to synchronise the QPRAMSS deliverables and the TWS1 “System Architecture” status by the end of each phase to avoid future conflicts.
3. to communicate this approach and sequence to all relevant TWSs and BWSs for achieving a common agreement as a starting point for working efficiently and cost-effectively together.
4. to support the other TWSs and BWSs with specific domain knowledge to understand the impacts of the other domains.

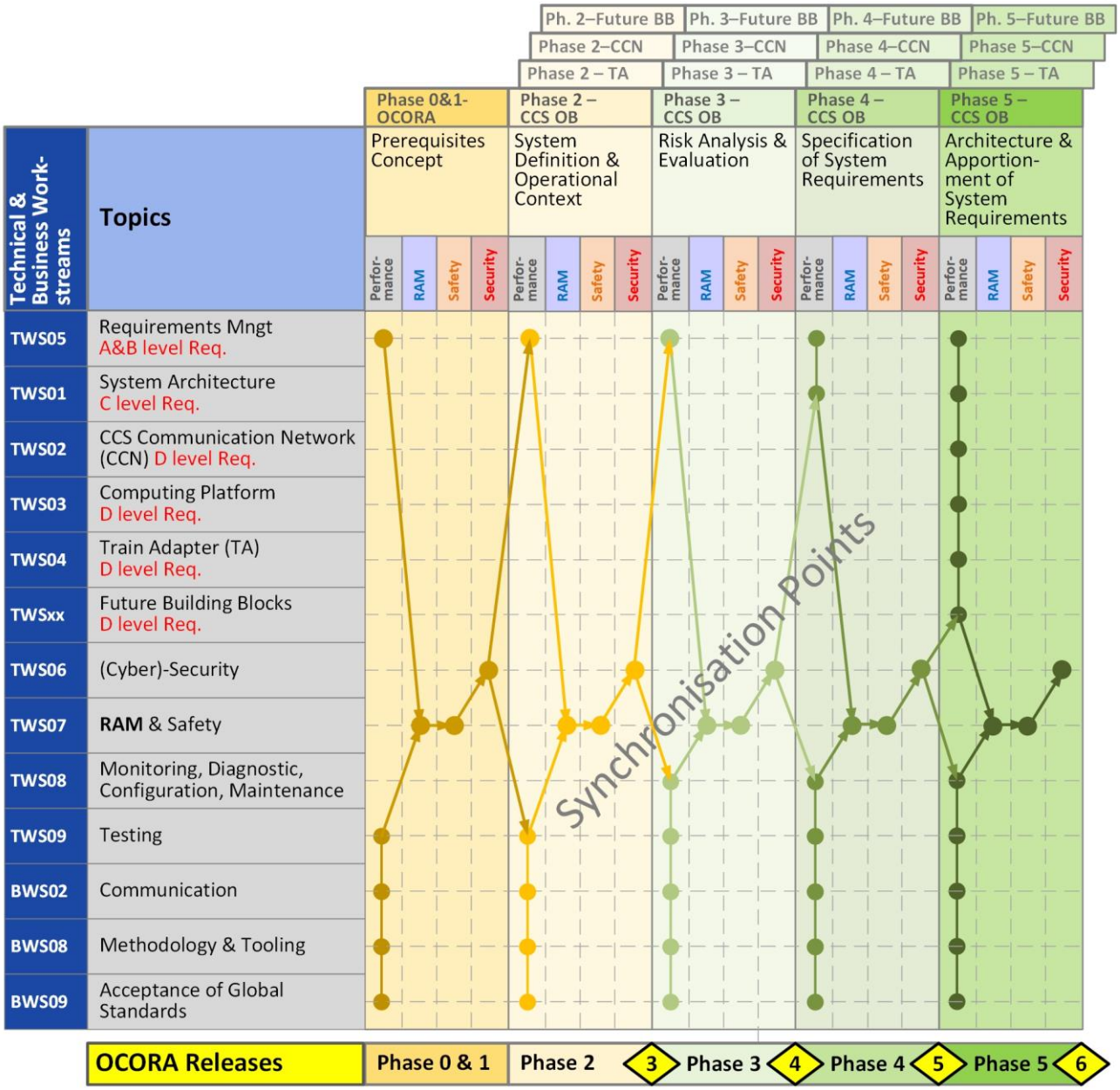

Figure 13 Break down of each phase into four sub-sections to ensure efficient fulfilment of all four aspects, i.e. Performance, RAM, Safety, and Security

4 RAM strategy to accomplish the RAM objectives

4.1 RAM

The RAM Strategy helps to define the RAM objectives. At the same time, Reliability, Availability, and Maintainability are strongly interlinked with each other. The RAM strategy focuses on Reliability and Maintainability, where the Availability is determined as a result. Secondly, as part of the RAM strategy, Human Factors and communication with all QPRAMSS domains will be included.

Therefore, the objective of the RAM strategy in the phase 1 to 5 is to:

- specify quantitative Reliability Targets,
- specify an approach for quantitative Maintainability Targets,
- specify an approach for qualitative process Reliability requirements, and
- specify an approach for qualitative process Maintainability requirements

as input for TWS01 “System Architecture” to design a functional architecture to be able to comply fully with the RAM requirements to be specified in phase 3, 4 and 5.

These quantitative and qualitative specifications are meant to be apportioned in part to:

- the supplier of the CCS, its constituents and the internal and external communication links and in part to,
- the organisation implements the CCS and its constituents.

The additional objective of this strategy includes, but is not limited to:

- specify an approach to apportion Availability targets to maintainer, logistics and supplier,
- sharing and learning from best practices in defining RAM targets and implementing CSS systems within organisation OCORA participants.

The specific activities within phase 0 to 5 are defined in the RAM Plan (part of the QRAMSS plan).

4.2 Life Cycle Cost (LCC)

The EN 50126-1 [7] promotes co-operation between the stakeholders of Railways in the achievement of an optimal combination of RAM, Safety and the related cost for railway applications. Besides

- functional requirements and
- technical requirements

contextual requirements, i.e. the relation between the system and the environment shall be qualified. This addresses issues such as:

- the system mission profile,
- maintenance and logistics,
- human factors (i.e. personal qualification),
- procedural environment, and
- costs.

RAM has a significant effect on the overall Life Cycle Costs (LCCs). LCC can be positively influenced during the first phases 1-5, to lower LCC as much as possible and to prevent that design changes must be made during the operational phase. Hence, the RAM Plan (part of the QRAMSS plan) shall include activities to estimate the Life Cycle Costs (LCCs) of the open onboard CCS.