Rail to Digital Automated up to Autonomous Train Operation

D36.1 – Demonstrator Specification

System Definition

Due date of deliverable: 30/11/2023
Actual submission date: 30/11/2023

Leader/Responsible of this Deliverable: Deutsche Bahn

Reviewed: Y

Document status		
Revision	Date	Description
01	20/04/2023	First Draft
02	07/08/2023	Conclusion on System under Consideration
03	28/08/2023	Actors, Functions, System Capabilities
04	06/10/2023	First internal Review
05	23/10/2023	Second internal Review
06	30/10/2023	Third internal Review
07	01/11/2023	Submission for TMT Review
08	30/11/2023	Updated version after TMT Review

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	x
SEN	Sensitive – limited under the conditions of the Grant Agreement [5]	

Start date: 01/12/2022 (WP36 kick-off 25+26/01/2023) Duration: 42 months

ACKNOWLEDGEMENTS

This project has received funding from the Europe's Rail Joint Undertaking (ERJU) under the Grant Agreement no. 101102001. The JU receives support from the European Union's Horizon Europe research and innovation programme and the Europe's Rail JU members other than the Union.

REPORT CONTRIBUTORS

Name	Company	Details of Contribution
Oliver Mayer-Buschmann	DB NETZ	Main author
Maik Fox	DB NETZ	Reviewer
Benjamin Labonté	DB NETZ	Reviewer
Martin Kochinke	DB Systemtechnik	Reviewer
Zahoor Ahmed	DB NETZ	Contributor Onboard Communication
Friederike Maier	DB NETZ	Reviewer
Kai Schories	DB NETZ	Contributor Diagnostics
Thomas Martin	SBB	Contributor on multiple topics
Rolf Mühlemann	SBB	Reviewer
Thomas Buchmueller	SBB	Reviewer
Wolfgang Wernhart	GTS	Contributor Safety and Modular Platform
Reinhard Hametner	GTS	Reviewer
Ulrich Geier	Kontron	Contributor FRMCS-Onboard
Manfred Taferner	Kontron	Reviewer
Henrik Larsson	Trafikverket	Reviewer
Harald Roelle	SMO	Reviewer
Thomas Bernburg	SMO	Reviewer

Disclaimer

ABBREVIATIONS AND ACRONYMS

Abbreviation	Definition
ATO	Automatic Train Operation
APS	Advanced Protection System
CBO	Common Business Objectives
CCS	Control-Command and Signalling
TCS	(System Pillar) Train Control and Supervision
DR	Digital Register
DSD	Digitale Schiene Deutschland
ERJU	Europe's Rail Joint Undertaking
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EULYNX	European initiative by 14 Infrastructure Managers to standardise interfaces and elements of the signalling systems
FA	Flagship Area (1 or 2) of ERJU IP
FP	Flagship Project (1 or 2) of ERJU IP
FRMCS	Future Railway Mobile Communication System
FVA	Functional Vehicle Adapter
GNSS	Global Navigation Satellite System
GoA	Grade of Automation
GSMR	Global System for Mobile Communications – Railway
IAM	Identity and Access Management
IM	Infrastructure Manager
IP	Innovation Pillar
IVV	Integration, Verification and Validation
MCx	Mission-Critical Services
MDCM	Diagnostics, Monitoring, Configuration and Maintenance
OCORA	Open CCS Onboard Reference Architecture
PKI	Public Key Infrastructure
R2DATO	Rail to Digital and Automated Train Operation
RAMS	Reliability, Availability, Maintainability and Safety

Abbreviation	Definition
RU	Railway Undertaking
SCI	Standard Communication Interface
SD	System Definition
SDI	Standard Diagnostics Interface
SEMP	System Engineering Management Plan
SIL	Safety Integrity Level
SMI	Standard Maintenance Interface
SuC	System under Consideration
SoW	Statement of Work
SRAC	Safety Related Application Conditions
SP	System Pillar
SysC	System Capabilities
SysF	System Function
TCMS	Train Control and Management System
THR	Tolerable Hazard Rate
TOBA	Telecom On-Board Architecture
TRL	Technology Readiness Level
TU	Train Unit
TSI	Technical Specifications for Interoperability
WP	Work Package

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

REFERENCES

Documents like standards, regulation etc. used in this document are listed at the end of this document in the References section.

Relevant and used terms, abbreviations, and acronyms are collected and listed in chapter 1.2.

1 INTRODUCTION

This “System Definition” document is part of the “Demonstrator Specification”, the first deliverable D36.1 of the R2DATO Onboard Platform Demonstrator work package. The purpose of a system definition document is to set the technical scope and purpose of the intended system, defining its environment, system boundary, system capabilities, system functions and interfaces. It points out needed assumptions and restrictions and sets the technical basis for further detailed specification work and analysis. It can be considered as a black-box specification on system level, without providing deeper sub-system design.

This System Description builds up the technical Demonstrator Specification together with two additional documents, the “User Stories & Test Cases” [3] and the “Architecture” [4] document. All three documents will be released as baselined versions in D36.1 but may be adapted later based on further specification work during the demonstrator’s consecutive Implementation Tasks 36.2-36.4 (month-10 to month-40 of the project). Potentially adaptions to this document may arise from possible project amendments, impacting insights from Sub-System Design decisions, and the results of the concrete realisation (Implementation, Integration, and Test) of the demonstrator during the project lifetime.

1.1 INSTRUCTIONS FOR READING

This document is addressed to the technically interested reader, and particularity to all parties involved in the development and implementation of the System under Consideration (SuC) that will be defined in the following chapter.

The R2DATO’s Grant Agreement [5] with its WP36 description is setting up the foundation of the demonstrator’s purpose, addressed topics and objectives. The “Statement of Work” (SoW) [2] renders and defines more precisely the planned activities, project roadmap, partner setup and concrete implementation plan. To gain a comprehensive project overview, it is recommended to study the SoW prior reading this System Definition. With this knowledge the document represents the best starting point to capture technical elaboration, followed by User Stories & Test Cases [3] and Architecture [4] documents that go deeper into the sub-systems based on the knowledge available and aligned between the partners.

Due to WP36’s nature of a demonstration project with a target TRL of 5/(up to 6)[1], the approach for developing the System Definition only follows basic paradigms of System Engineering standards as ISO15288 and can’t be considered as CENELEC-compliant. As an example, RAMS processes as mandated in CENELEC [23] are only partly foreseen, mainly towards security topics.

Other examples are the lack of an operational concept, limited pre-analysis of stakeholder demands and requirements. A concept of use and lifecycle model are as well not applicable and therefore a strict top-down approach for the system and sub-system design is not foreseen. Anyhow the nature of the followed approach is roughly illustrated in Annex A:.

---

[1] *"*TRL5 Pre-prototype tested in lab: *Integration of components with reasonable and realistic supporting elements for testing in a simulated environment. High fidelity is achieved in laboratory."*

*"*TRL6 Prototype tested in relevant environment: *The technology is tested in a relevant environment. It starts to be considered as a representative prototype to be tested in a high-fidelity laboratory environment or in a simulated operational environment".*

The document starts with the conceptual chapters on the system's context, scope, purpose, and its environment. The subsequent chapters focus on the system definition aspects, defining the system boundary, introducing the system capabilities and functions, addressing operational conditions and scenarios. Any specific implementation and commissioning activities covered in this document are only superficial and are only meant to represent a guideline towards the respective activities to be covered in later specification activities within the Implementation Tasks 36.2-36.4 of the project.

1.2 TERM DEFINITIONS

The terms outlined in the table below will be used throughout the document. The list is being populated using currently available ERJU System Pillar definitions, terms introduced in other R2DATO WPs or public available sources, such as rail initiatives.

In the context of the system definition for the Onboard Platform Demonstrator, these terms are to be aligned with prior work, e.g., from OCORA and Shift2Rail to ensure a European wide understanding.

Term	Definition
Functional Application	A comprehensive set of self-contained software functions, assumed to be provided as one product by a single vendor. A functional application could consist of: - 1..n software functions and - a generic (deployment) configuration.
Modular (Computing) Platform	Modular Computing Platform refers to an environment, that allows building and running Functional Applications. It comprises of hardware and software (i.e., the Runtime Environment and the necessary tools for development, testing, integration, etc.).
Safe Runtime Environment (RTE)	Software Environment on which functional applications are executed on top of an API, ensuring their separation. The RTE provides explicit communication methods and services towards functional applications up to Sil 4. It is a component of the Modular (Computing) Platform.
Functional Vehicle Adapter	Functional Vehicle Adapter is a software function that provides a Standard Communication Interface (SCI) from a train specific TCMS towards the CCS applications for vehicle functions and vehicle information services as a configurable conversion logic with the objective to reduce migration and integration costs of CCS-Onboard systems for existing vehicles.
CCS Onboard	The CCS Onboard (system) comprises functions related to the Onboard European Train Control System, in the context of the demonstrator selected demo applications realised on the Modular (Computing) Platform.
Train Adapter	The Train Adapter enables the integration of a CCS Onboard System into existing train's. It typically includes wired signals and if necessary supports different network types. In the context of the demonstrator, a physical realisation is out of scope, but software functions will be evaluated and demonstrated, in particular the TCMS Data Service and the Functional Vehicle Adapter.
Diagnostics, Monitoring, Configuration and Maintenance (MDCM)	MDCM shared services, potentially provided to multiple onboard domains, e.g., for remote diagnosis purpose and software update.

Onboard FRMCS System	The FRMCS Onboard System provides communication services via capabilities of the Transport Domain to and from onboard applications / entities. The Onboard FRMCS system includes a Gateway Function providing interfaces to the train applications and a Radio Function.
FRMCS Onboard Gateway	The Onboard Gateway is responsible for the coordination and managing of access to the FRMCS transport services offered by the FRMCS system.
FRMCS Trackside	FRMCS Trackside is a lab representation of trackside FRMCS functional entities of a FRMCS network.
FRMCS Trackside Gateway	The FRMCS Trackside Gateway provides access to communication and supplementary services supported by the FRMCS System to and from trackside applications.
Safe Demo Application	A native SIL4 application showing an ETCS control loop involving bi-directional communication over FRMCS and with TCMS and diagnosis to show safety relevant functionality.
Basic Integrity Demo Application	A native basic integrity application showing an ATO control loop involving bi-directional communication over FRMCS and with TCMS and diagnosis to show non-safety relevant functionality.
Onboard Communication Network	Realisation of standardised and seamless communication among on-train domains, connecting the different functional domains as TCMS, CCS, operator and customer-oriented services based on a common network technology (ISO OSI Layer 1-6)
Shared Services	Shared Services comprise such services, that get potentially shared over multiple Onboard domains in the future, e.g., if there exist a common onboard communication network. In the farer future there may exist standardised shared diagnosis (MDCM), time and localisation services, etc.
Security Services	Security Services comprise controls and functionalities to ensure a secure operation, examples are Identity and Access Management and Intrusion Detection.
TCMS data	A means for applications to use information generated in a given TCMS environment, in a uniform way, and not depending on the application itself or its environment.
TCMS Simulation	A TCMS Simulation is a representation of TCMS Systems (e.g., door and brake control units and their data models, providing data status information of simulated assets).
TCMS Data Service	An approach to realise TCMS formalisation, the definition and demonstration of methods for a generic TCMS data model and service interface (for communication and control) and for particular use cases, e.g., Doors, Brakes or HVAC. Definition and application of methods to formalize the semantics of concepts and entities related to system status information, data services, and operational diagnostics.

Table 1 – Table of Definitions

2 SYSTEM UNDER CONSIDERATION

2.1 SuC Purpose and Scope

The rationale behind the definition of the System under Consideration (SuC) of the WP36 is derived from the primary goal to combine a subset of selected Technical Enablers from the cluster Enabling Digital Technologies in a prototype project and to demonstrate the feasibility in a first technical realisation focused on Onboard Platform technologies. This functionality allocated in the SuC is further defined in subsequent sections. The main motivation can be summarised as:

- Implement an overall onboard platform reference deployment on which exemplary safe and basic integrity (BI) applications are integrated in a lab environment.
- Implement related specifications to pave the way for modular platforms, their certification and homologation.
- Investigate how the selected onboard platform concepts and solutions work together as a starting point for future modular deployments.

The following points provide an overview on what shall be achieved by the development of the SuC and what is not covered.

2.1.1 Goals for the definition and development of the SuC

- A starting point towards a system architecture - including the definition of interfaces based on the alignment among the project partners and available input from the SoW and other R2DATO work packages and from the System Pillar.
- The definition of a set of system capabilities.
- The definition of a set of potential system and actor functions.
- The identification of potential Functional Clusters that can be combined to comprise the SuC.
- The integration of potential Functional Clusters within delivered units for validation and verification of the technologies to be developed.
- The integration of identified and selected Technical Enablers to the SuC with the intention to demonstrate their technical feasibility and their benefits.
- Prove usefulness and applicability of a standardized platform API to develop safe and basic integrity applications.
- Prove of common and basic concepts (defined in the use-cases) using a generic platform approach related to a standardized API.

2.1.2 Not covered by the definition and development of the SuC

- The development of operational scenarios (rather in the responsibility of System Pillar, corresponding work has for example just started in the SP Computing Environment domain)
- The development of full and comprehensive functional onboard rail applications, as the focus of the demonstrator is the realisation of technical enablers in the area of platform technologies. Full features applications may be realised only in case that a dedicated application supplier will join the partner setup, which is not the case yet.
- The development of TCMS functionality and TCMS components will only be simulated and mocked-up since no TCMS supplier is available in the partner setup yet.
- Development of wayside functionality and infrastructure is only mocked-up for demonstration purpose.

- Elaboration of the system's contribution to the operational needs has rather been identified as part of the deliverable D36.5 (Onboard platform blueprint for later EU- RAIL phases established and disseminated)

2.1.3 Relevant Functional Clusters

The following diagrams provide a high-level view on functional clusters as already introduced in the R2DATO Grant Agreement [5]. The relevant clusters are identified by red boxes and serve as a first demarcation idea for the later specified SuC and its system boundary.

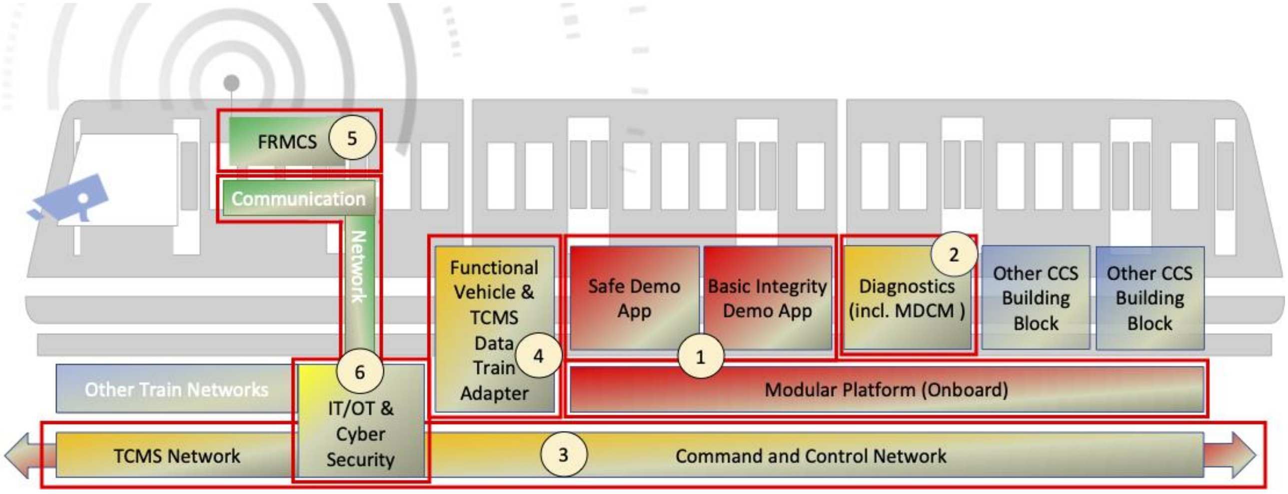

Figure 1 – Introduction to the relevant Functional Clusters

Since other onboard domains (e.g., Operator, Passenger) are out of scope, they are represented here as “Other (Train) Networks only” without building a relevant Functional Cluster. The same applies to additional building blocks (of the CCS Onboard domain), represented by the two blue coloured boxes. The demonstrator identifies and realises a set of demo applications that serve as a representative selection providing relevant realisation examples for both, safety and basic integrity functions. More extended and full feature implementations and integration of exemplary production grade Onboard CCS applications may be realised in later phases of R2DATO. The MDCM is visualised on top of the Modular Platform, which should only be considered here as one potential deployment option. Physical deployments are not covered in this document, they will be evaluated in the Physical Architecture chapter of the Architecture [4] document. The development and commissioning of the SuC is performed in later Implementation Tasks (36.2 - 36.4), including sub-system design and documentation.

A simplified view on the functional clusters that are in the focus of the project is provided by the following Figure 2. This representation will be adopted and populated with actors and interfaces in the following chapter of this document. TCMS and wayside entities are shown for completeness only since some of their functions are relevant for the demonstration as external actors towards the SuC.

Functional clusters that are visualised here as dashed boxes imply that only smaller subsets and functions are realised in the project or that their realisation may reach a slightly reduced TRL of typically 5 or even less. As an example, the realisation of a Train Adapter will potentially be restricted due to the absence of a contributing solution supplier from the industry. Please refer to the chapter 2.4.3 for details.

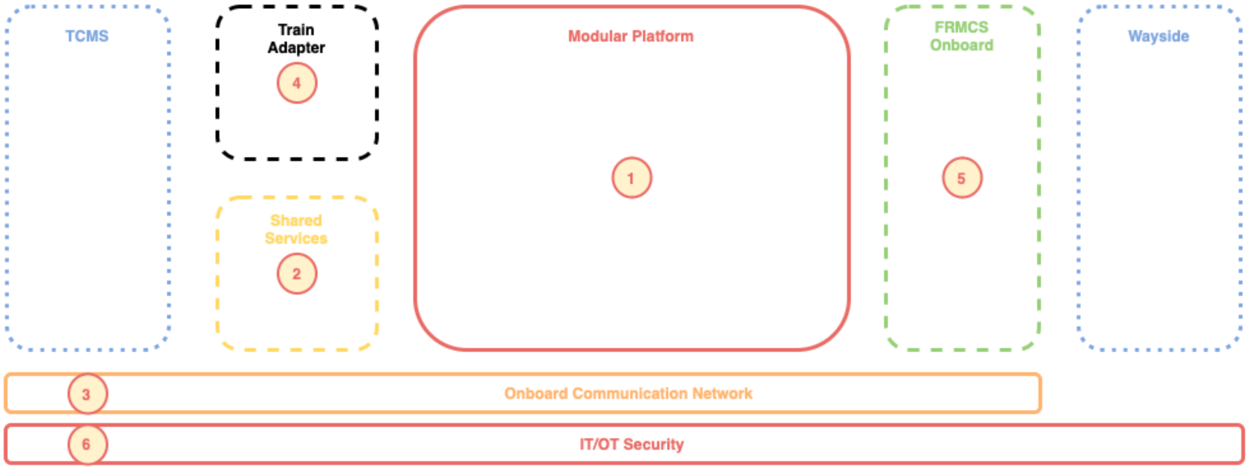

Figure 2 – Simplified view on relevant Functional Clusters

The numbering scheme corresponds to the following table, that reflects a record of the functional clusters, their scope and identified system capabilities. More details on each system capability will be provided in chapter 3, explaining their motivation, needs, input, output, and relations to corresponding actors, defining relevant interfaces, and functions.

It must be pointed out that many of the subsequently introduced system capabilities are derived from former work of initiatives introduced in chapter 2.2.1 and operational knowledge and experiences of the participating partners.

A dedicated operational concept, stakeholder needs, and stakeholder requirements analysis cannot be performed in depth in the context of this demonstrator project. The demonstrator's system capabilities are tailored based on user stories that have been defined during Task 36.1 between the participating partners. Concrete input from WP 5 (Automation Processes Use Cases and User Requirements) may be considered in future iterations and adjustments of the project if feasible and necessary. The same applies to output from the System Pillar.

It must be noted that the following System Capabilities do not reflect those that might be defined in the System Pillar based on architectural work, e.g., in the Train-CS domain.

The term "System" or "System under Consideration (SuC)" in the context of WP 36 reflects the Onboard Platform Demonstrator's System of Interest. The System Capabilities introduced in this document represent a selection that fits to the objectives and goals defined in the Grant Agreement [5]. They shall demonstrate feasibility and serve as a foundation for future work and follow-up phases of R2DATO, dealing with the limitations that arise from available resources of the WP's participating partners.

The following allocation matrix provides an introduction and overview to the six identified Functional Clusters and a mapping to the set of system capabilities that get in detail explained in chapter 3.2.

Specified Functional Cluster	***Scope***	***System Capability***															
		SysC_01	***SysC_02***	***SysC_03***	***SysC_04***	***SysC_05***	***SysC_06***	***SysC_07***	***SysC_08***	***SysC_09***	***SysC_10***	***SysC_11***	***SysC_12***	***SysC_13***	***SysC_14***	***SysC_15***	***SysC_16***
1. Modular Platform	*Standardised hosting of basic integrity and safety applications independently from underlying hardware.*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*x*	*(x)*	*x*
2. Shared Services *(introduced as “unified diagnostics services” in the Grant Agreement*[5]*)*	*Realize a holistic concept for Onboard diagnostics, monitoring, configuration, and maintenance services, their interfaces and datasets. Services that are shared and used from different clusters as Time Service, Network Services, Configuration, Monitoring Maintenance and Diagnosis (MDCM)*	-	*(x)*	-	-	*(x)*	-	*x*	*x*	*(x)*	*(x)*	*x*	-	-	-	-	-
3. Onboard Communication Network *Focus: CCS, TCMS*	Realisation of standardised and seamless communication among on-train domains and dedicated demonstrator components, based on a common network technology (ISO OSI Layer 1-6). Main scope of the demonstrator is the take over from WP 23 results and realisation of communication functions, including FRMCS.	-	*x*	*(x)*	-	*x*	*(x)*	*x*	*x*	*x*	*(x)*	*x*	*x*	*x*	*x*	*x*	-

Specified Functional Cluster	**Scope**	**System Capability**															
		SysC_01	**SysC_02**	**SysC_03**	**SysC_04**	**SysC_05**	**SysC_06**	**SysC_07**	**SysC_08**	**SysC_09**	**SysC_10**	**SysC_11**	**SysC_12**	**SysC_13**	**SysC_14**	**SysC_15**	**SysC_16**
4a Train Adapter Focus: Functional Vehicle Adapter	*Enable the integration of standardised interfaces between the TCMS and CCS domains for existing vehicles (and designs) towards future CCS Onboard solutions.*	-	(x)	-	-	(x)	-	-	x	(x)	-	-	-	x	-	-	-
4b Train Adapter Fucus: TCMS Data Service	*Provision of TCMS Data in a harmonised way, independent from the actual vehicle implementation.*	-	(x)	-	-	(x)	-	-	x	(x)	-	-	-	x	-	-	-
5. FRMCS Onboard	*FRMCS link between Onboard and Wayside Applications*	-	x	(x)	-	x	(x)	(x)	-	x	(x)	x	x	-	x	x	x
6. IT/OT Security	*Security Services comprise controls and functionalities to ensure a secure operation. The scope of the demonstrator is secure communication, identity and access management and secure operation of the demonstrator assets.*	x	x	-	-	x	-	x	x	x	x	x	x	x	x	x	-

Table 2 – Functional Clusters and System Capabilities

2.2 SuC Context

This chapter provides an overview of the projects and activities that are relevant for the definition and development of the SuC.

2.2.1 International Harmonisation

2.2.1.1 Europe's Rail Joint Undertaking (System Pillar and Innovation Pillar)

Europe's Rail Joint Undertaking (ERJU) aims at creating a uniform approach across Europe for the harmonisation of Railway operations. In order to perform this, it brings together Infrastructure Managers (IMs), Railway Undertakings (RUs) as well as industrial partners and organises the work within two work areas: the System Pillar (SP) and the Innovation Pillar (IP). The task of the SP is to consolidate the work that predates the start of the ERJU project and formulate a common specification basis to be proposed as addendums to the existing interoperability specifications. The IP is more focused on the technology development, exploration of different architectures and implementation of prototypes for testing the feasibility of various proposals. As such, the combination of the two Pillars forms a comprehensive effort to align and standardise the railway of the future on a European level.

2.2.1.2 Shift2Rail

Shift2Rail (S2R) aims to bring to conclusion the research and development of some key technologies to foster innovations in the field of railway signalling, automation, telecommunication, testing methodologies and Cyber Security, as part of a longer term Shift2Rail IP2 strategy towards a flexible, real-time, intelligent traffic control management and decision support system.

There were a couple of commercial projects in S2R such as X2Rail-1 to X2Rail-5 which were focused on different technical demonstrators for future Railway functions such as Moving Block, ATO, Adaptable Communication System, Virtual Coupling and Train Integrity. Further projects such as Linx4Rail and Linx4Rail2 were focused on the modelling of the overall Railway architecture whereas TAURO was looking mainly for the Remote Driving function.

2.2.1.3 Reference CCS Architecture

The ERTMS Users Group (EUG) founded an initiative for European Infrastructure Managers (IM) for a Reference CCS Architecture (RCA), based on results of the Swiss programme SmartRail-4. The aim was to provide a reference architecture including requirements for behaviour for domains like Traffic Management, Automatic Train Operation and Trackside Route and Train Protection. When it became clear that ERJU would be a joint European activity amongst Infrastructure Managers and Signalling Vendors, the initiative was finished with release 1.0 [9]. Several concept papers have been published which serve as an input in the pre-project of ERJU. These documents are supposed to also become a base for the specification of the Onboard Platform Demonstrator.

2.2.1.4 OCORA

OCORA, the “Open Control, Command and Signalling On-board Reference Architecture” initiative, aims to reduce life-cycle costs and facilitate the introduction of innovation and digital technologies with standardized interfaces by establishing a modular, upgradeable, reliable, and secure CCS on-board architecture. OCORA deliverables are published under the European Union Public License (EUPL) and are consequently available for all stakeholders.

Today’s deployed CCS On-Board systems are proprietary and vendor specific solutions, creating a dependency to the specific vendors.

The OCORA architecture introduces a generic platform concept where core CCS functions can be realised on a generic platform that enables adding, removing or changing functional applications without affecting the computing platform or runtime environment on which they are installed or the state of approval of non-affected parts of the system, e.g., unchanged functions. This will facilitate fast and easy software updates and upgrades of only those applications for which that is necessary, e.g., when requirements demand frequent updates of security software. Safety and non-safety critical applications shall be able to coexist on the same platform and may even run on the same computing hardware.

2.2.1.5 EULYNX

EULYNX is a European initiative by 15 Infrastructure Managers to standardise interfaces and elements of the signalling systems. It is aiming for defining and standardising interfaces in the future digital control command communication, signalling and automation systems.

The project was started in 2014 and has evolved in 2017 into a standing organisation for standardisation of interfaces. The goal of EULYNX is to establish a universal and international standard that forms the foundation of a future CCS Architecture for efficient and harmonized operations and significantly reducing the lifecycle cost for signalling systems.

It has recently been integrated in the development work of the ERJU System Pillar.

2.2.2 National Projects

2.2.2.1 Digitale Schiene Deutschland and Digitalisierung Bahnsystem

The “Digitale Schiene Deutschland” (DSD) aims at a fundamental modernisation and digitalization of the German Railway infrastructure to enhance the capacity, quality, and efficiency of the railway system. It aims at a target picture in which trains run automated, at an optimal distance, and are steered optimally throughout the railway network. The introduction of applications for this target picture is enabled by the rollout of ETCS L2 and L3 (Combined in later ETCS baselines). The platform technologies and technical enablers involved in the SuC belong to key building blocks of the future railway system. The first prototypes of the group of clusters represented in the DSD target picture would be through the ERJU SP and IP activities.

2.2.2.2 SmartRail 4.0

SmartRail 4.0 was a program of the rail sector, initiated by the Swiss railways for the comprehensive modernisation and automation of the essential railway operating processes. The focus was on the end-to-end digitisation of the modern railway of the future. Central to the vision of the future railway system was the concept of a "geometric interlocking" and the locating of the train front and end as pioneering achievements. Further future-oriented technologies such as FRMCS, standard interfaces in both - the infrastructure and rolling stock - were part of the technical-operational target system of the participating Swiss railways - this development was also intended to create the space for the recognized necessary paradigm shift in previous ways of thinking and planning in the railway sector. The Swiss railways have developed many concepts and feasibility studies to investigate the benefits, costs and working principles of this new railway system.

2.3 SuC Environment

2.3.1 Identification of inputs and dependencies

The following list shall identify inputs and dependencies on the SuC. A more detailed view on concrete input and deliverables is available in the timeline and implementation plan chapter of the SoW [2].

2.3.1.1 Technical enablers, corresponding R2DATO work packages

The following R2DATO work packages have an impact on the WP36 work. First deliverables have been collected from other sources as Shift2Rail and other initiatives as well.

- IT/OT Security, Cybersecurity Framework (WP3 Task 3)
- Onboard Communications (WP23)
- Connectivity Development – FRMCS (WP25)
- Modular Platforms Specifications (WP26)
- Further enablers, (e.g., Digital Register WP27, if applicable for Onboard)
- TCMS Data Service (WP31.2)
- Testing, Validation and Certification (WP34, WP35)
- R2DATO deliverables from WP1, WP2, WP3, WP5, WP6 and WP8 may influence the project as well

2.3.1.2 System Pillar domains and standardisation activities

The following System Pillar domains and standardisation activities in particular have a major impact on the work in WP36, the list may not be complete:

- OCORA architecture and prior work on Safe Computing Platform (to be continued in SP)
- SP Task2 Computing Environment domain
- Standardisation work on FRMCS (especially TOBA)
- SP Task2 Train-CS domain
- SP Task2 Transversal CCS Components domain
- Train integration concept from OCORA - Functional Vehicle Adapter (FVA)
- SP Architecture domain
- SP PRAMSS domain
- Technical Specifications for Interoperability and corresponding Subset specifications in focus

The results of the demonstrator on the other hand will influence future work in R2DATO. The research and feasibility on platform technologies is supposed have an impact on future work in the System Pillar, e.g., on modularity concepts and towards the incorporation of the evaluated technologies into the TSI input plan. Further elaboration on potential impact is contained in the document Demonstrator Specification.

2.3.2 Support of existing Interface specifications

The SuC shall follow existing standards and interface specifications. But it shall be noted that this applies only towards their applicability and the degree of the demonstrator's target TRL. An example of such an existing specification is the UNISIG SUBSET-147 V1.0 (SS-147) for the Onboard Communication Network that will be considered for the system definition, as it is classified as a mandatory specification in the latest TSI 2023 for new developed vehicle designs, requiring first authorisation. The SS-147 currently covers the lower layers of the network ISO OSI stack and shall be extended during the project lifetime to layers 1-6.

For Modular Platform specifications the specification situation is similar. The available initial specification D26.2 can be considered as in a very early-stage and the next publicly available deliverable is foreseen for month 24 (October 2024) [11]. Specification updates will have a major impact on the Onboard Platform Demonstrator implementation and its realisation tasks and may become available too late to be considered in an appropriate way.

Since a baseline of relevant specifications is not available at this point in time, assumptions must be made in some parts. The project success highly depends on a stable overall R2DATO planning. The availability of targeted results from other R2DATO work packages and input provided by the System Pillar is the key and relevant content must be provided in an appropriate and needed quality.

2.3.3 Legislative and Economic Issues

The regulation of the Grant Agreement [5] apply to the development of the system and define the contractual foundation for WP36. Amendments haven't been foreseen so far but might happen if needed in the future.

Economic issues as limited resource allocation and absence of partners contributing to specific areas (e.g., lack of application and solution suppliers), add challenges and risks to the project and may result in needed adjustments during the implementation tasks.

2.3.4 Previous systems

The SuC is a combination of existing technologies and new development with a novel technical approach compared to existing railway systems. There do exist systems that can be used as a reference system in the RAMS analysis and for operational inputs and aspects of the SuC.

2.3.5 Similar systems

The SuC aims to pave the way for novel approaches, the realisation for modular system architectures and new technologies, extending but as well replacing currently deployed onboard solutions. There does exist a high probability that functional and non-functional aspects of the SuC will overlap with those existing solutions. The Onboard domain must be considered as a brown field environment, providing a superset of specifications, requirements and frame conditions that must be considered.

2.3.6 Previous RAMS requirements and performance of similar systems

As availability and reliability figures can vary heavily depending on the concrete product, it cannot be stated as a simple number/requirement. Therefore, a certain variability is required here. This translates into support of different redundancy/availability models, ideally switched only by configuration. Classical and well-known approaches are to support composite fail safety, e.g., with 2oo3, nx2oo2 or similar configurations.

Depending on the redundancy/availability model, maintenance and operation will be influenced. E.g., a 2oo3 systems would allow uninterrupted exchange of a defect hardware, 2oo2 would always require a reboot of the system.

Regarding performance, usual start-up times of the modular platform should be in the order of 30 seconds to 2 minutes. Similarly, reaction times of the system ("end-to-end") should be in the order of 500ms to 1 second, tendency to even faster reaction, dependent on the railway application. Internally (inside the platform), this would require synchronisation periods in the order of 5 - 20ms.

The required Tolerable Hazard Rate (THR) for the railway applications which will be run on the modular platform shall be derived from a hazard analysis. For each hazard, the relevant standards ([EN 50126-2] chapter 10.2.2 / [EN 50129] A.4.3.2) impose system level safety requirements for a THR. Those requirements are then considered given a specific functional composition of the overall system, where the composition is based on the system architecture. The modular platform is a generic product, and no specific safety function can be allocated without a particular application context. A safety function can be realized by combining several modular platform applications. Based on the tolerable functional (unsafe) failure rate, a Safety Integrity Level (SIL) is derived. In case of the modular platform SIL 4 is required. Note that it is the responsibility of the application that its function is developed according to the correct SIL. However, the application can rely on the modular platform services to have an integrity with SIL 4.

2.3.7 Safety Legislation

The following applies to a railway system including safety functions, and not for this demonstrator.

For safety-relevant changes to railway systems (e.g., technical, operational, regulative or organizational changes), the risk assessment process in accordance with EU regulations 2015/1136 and 402/2013 (CSM-RA) must be applied.

However, technical changes to a system that are handled with the RAMS management process of the CENELEC standard EN 50126 (+128/129) are generally compliant with the CSM procedure.

Nevertheless, it is a necessary, that each change in the “safety chain” of a system function needs to be considered in a safety case and assessed, ultimately. Depending on the modularity and rules of the underlying systems (RTE, Virtualisation, etc.) this process can be lightweight up to very heavy. Therefore, a dedicated use case or other investigation on that topic would be helpful.

2.3.7.1 Safety Requirements

Applicable Safety Requirements can be taken from the CENELEC Standard EN50126:

- Functional Safety Requirements

  EN50126-2 (9.3.2.)
- Technical Safety Requirements

  EN50126-2 (9.3.3.)
- Contextual Safety Requirements

  EN50126-2 (9.3.4.)

Practically, using a certain specific standardised platform would mean to fulfil all Safety Related Application Conditions (SRACs) as the assessment of the platform is based on their fulfilment. The number of SRACs should be as low as possible, and it would be ideal, if different platforms (different vendors) would share as many SRACs as possible. Nevertheless, it is not realistic to assume, that different platforms can share the exact same set of SRACs. Further work on that topic is to be expected in R2DATO D26.4 [12].

2.4 Constraints on the System Solution

There exist multiple constraints that will affect the architectural design of the system and the means to realize it, e.g., the absence of appropriate application and TCMS solution suppliers and limited resources for the WP 36.

Additional constraints arise from parallel ongoing specification work and needed progress in relevant R2DATO work packages and SP activities.

2.4.1 Modularization and system architecture in System Pillar

The Onboard Platform Demonstrator supports the architectural work on modularization and definition of building block concepts for CCS-Onboard systems by providing feasibility and evidence in their realization, making sure that the realized SuC is fitting to that purpose and environment. At this point in time there do not exist publicly available deliverables based on this a top town approach from operations to system and sub-system level. Nevertheless, direct exchange between R2DATO WP36 and the corresponding SP domains (Architecture, Computing Environment and Train-CS domains) is key and will be performed regularly to ensure alignment. As well the SP is motivating and promoting the modularization of the CCS onboard system and bottom-up approaches - as foreseen as well - may provide earlier architectural results and guidance.

2.4.2 Impact of specification absence

Many specifications that must be considered as direct input are incomplete, marked as “for further study” or even need to be considered as early drafts. A common and complete consistency report and baseline of relevant specifications in not available yet. Corresponding work is ongoing in WP3 on a “baseline zero,” that will mainly follow the purpose to identify the status quo in R2DATO, the main dependencies between R2DATO work packages and available and planned inputs from and to the System Pillar. The definition of processes for the interaction and exchange between Innovation Pillar and System Pillar is still ongoing, respective work on Processes in R2DATO is performed in the WP4, WP5 and WP6.

The main risks identified for reaching the goals of the demonstrator are the status of:

- FRMCS standardization, its roadmap towards a complete FFFIS (Form Fit Function Interface Specifications) specification
- Modular platform and Computing Environment specification input, please refer to D26.2 [10]. The foreseen inter exchange between the specification activities and their direct implementation in WP36 and feedback towards WP26 are a challenging task.
- Parallel activities in SP Computation Environment domain shall identify the system's contribution to the operational needs. It is expected that developed results will support in both directions.

2.4.3 Arising assumptions and limitations

The results of the activities and alignments between the partners during the specification phase shall be documented and include any assumptions and justifications.

The following table provides a record of assumption that have been made during alignment in Task 36.1. Further assumptions may be needed and added in later phases of the project.

Number	Assumption Text	Comments	Status
As01	**Train Adapter and Functional Vehicle Adapter** Neither the Functional Vehicle Adapter (FVA) nor a dedicated Train Adapter (hardware) solution might be implemented or integrated in WP36 Implementation Tasks (36.2-36.4). The current assumption is (at the time of Task 36.1), that related components will be considered in the system architecture as conceptional only, resulting in related elaboration during the dissemination Task 36.5. Therefore, the target here is TRL2, a higher TRL might only be achieved in case the WP36 partner setup can be extended later by an additional partner from the R2DATO participation list.	The interfaces between the TCMS and CCS domain will be considered on conceptual level only since the actual reserved resources for the topic a very limited and corresponding SUBSET specifications are still under development. Pre-work on the FVA concept is available in OCORA [21]. We encourage suppliers to step in and provide an implementation.	Open
As02	**FRMCS** The Demonstrator Setup focuses on FRMCS Onboard components. Needed FRMCS Trackside and Network infrastructure will be provided from Task 36.3 in a dedicated FRMCS lab by Kontron. The final laboratory setup will utilise FRMCS mock-up. The realisation of a 5G based airlink and fully developed FRMCS network infrastructure is out of scope of the demonstrator.	Other projects cover those topics and hence are not in focus of the WP36.	Open
As03	**Targeted TRL**: The Grant Agreement[5] targets a TRL of 5/6 for the demonstrator. Since the demonstrator aims to integrate multiple technical enablers and platform technologies to investigate how different onboard platform concepts work together, while resources are limited, the current assumption is that many of the solutions realised in the project might rather reach a maximum TRL of 5.	Since the hosted applications are mainly demo applications, they are candidate for lower TRL, while the modular computing platform hosting them shall reach a TRL of up to 6. Mock-Up components and simulations (outside the SuC) will be of lower TRL.	Open
As04	**Implementation plan**: The realization of functionalities relies on the availability of relevant specifications. Currently there is awareness that there exists a high risk for delays, incompleteness, and potential low maturity of those specifications. The current assumptions and implementation plan is based on "delivered as planned".	Please refer to the SoW chapter 2 for more details.	Open

Number	Assumption Text	Comments	Status
As05	Real TCMS Systems won't be integrated into the demonstrator lab setup but replaced by simulations, since they are out of scope and due to the absence of a TCMS system suppliers in the work package.		Open
As06	FRMCS environments consists of onboard and trackside infrastructure, realising bidirectional Onboard to Wayside communication compliant to the new Railway Mobile Communication standard. FRMCS standardisation is still in full activity and will not be finalised during the project timeline. Many parts of the specification are still marked as "for further study" which adds some degree of uncertainty to the envisioned implementation results.	In the respect of the FRMCS Onboard realisation, the focus in this project is not wireless communication technology but the integration of FRMCS software and services towards the Modular Platform.	Open

Table 3 – Assumptions Made for WP36 System Definition

3 SYSTEM DESCRIPTION

3.1 SYSTEM BOUNDARY

This chapter defines the boundaries of the SuC as a whole. The System Boundary is defined by the following aspects:

- A system context diagram, showing the System Under Consideration (SUC) and all system actors the SuC interacts with.
- Enumeration of all actors, definition of the attributes of each actor.
- System interface descriptions introducing the most relevant external interfaces.
- Tables with attributes for each interface.

Figure 3 illustrates the distinction between the proposed System Boundary mapped to the Functional Cluster views and the potential demonstrator setup.

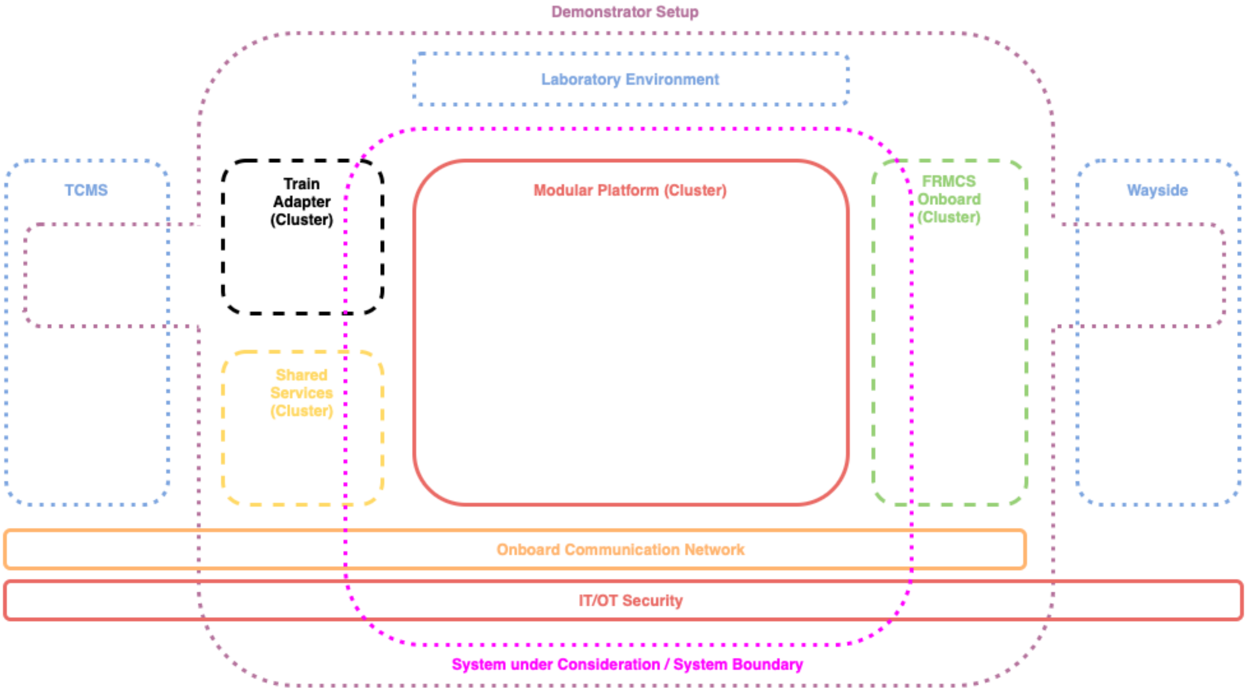

Figure 3 – System under Consideration vs. Demonstrator Setup

Figure 4 depicts the context of the Onboard Platform Demonstrator SuC, showing its main external actors and systems that interact with the SuC. Most actors represent technical systems, the human actors on the right-side are rather relevant in an operational context of the SuC. All those external actors will be in detail described in chapter 3.1.1 including additional information as their type, rationale, allocated actor functions and interfaces.

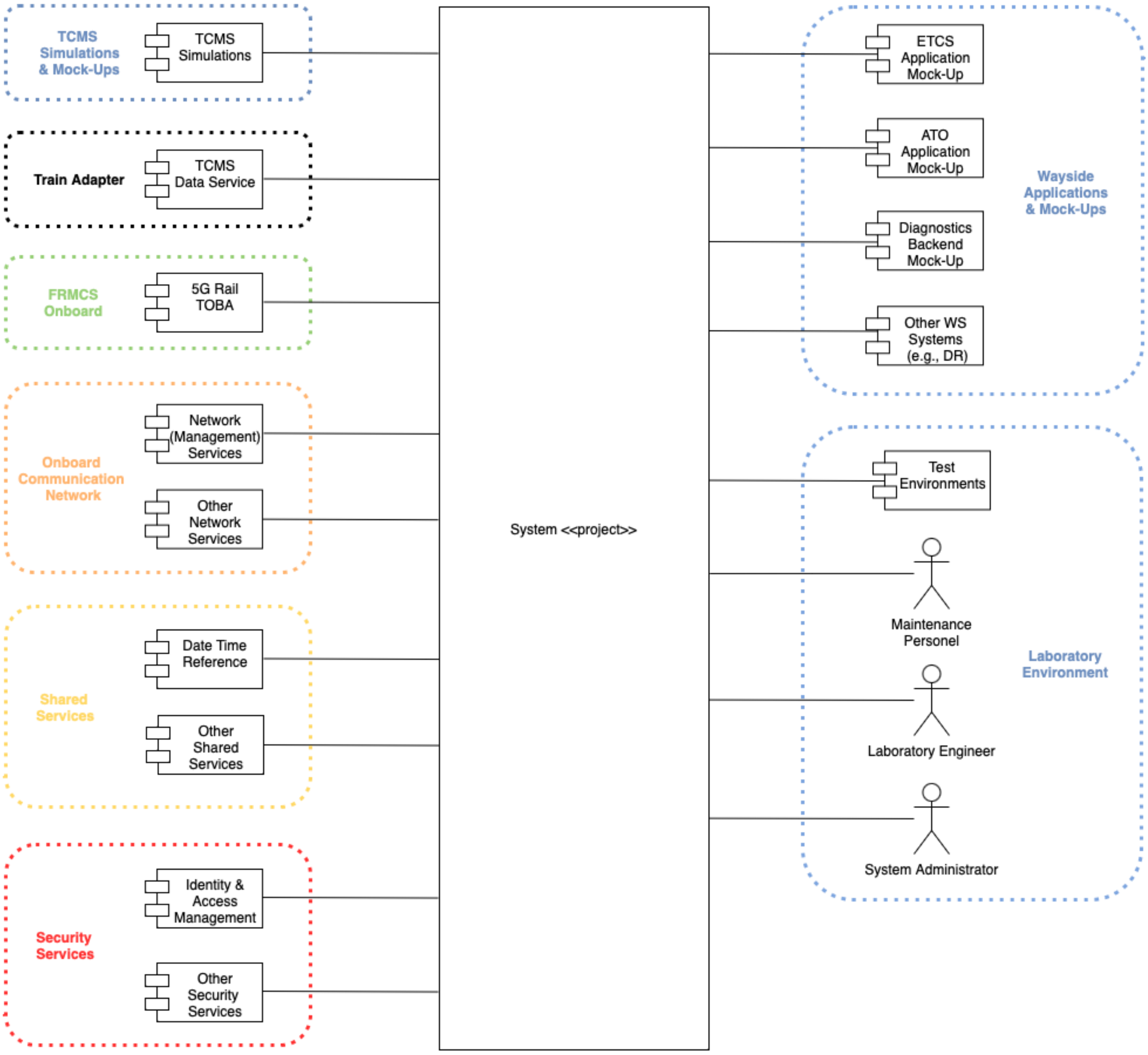

Figure 4 – System under Consideration, System and Human Actors

3.1.1 Actors

3.1.1.1 TCMS Simulations

Attribute	Content
Name	TCMS Simulations
Description	Train Control and Management System, in the demonstrator setup rather a pure simulation-based solution.
Type	External System
Rationale	A representation of TCMS Systems (e.g., door and brake control units and their data models, providing data status information of simulated assets). Real TCMS Systems won't be integrated into the demonstrator lab setup but replaced by simulations, since they are out of scope and due to the absence of a TCMS system supplier in the work package. TCMS data is needed to demonstrate parts of the Train Adapter and diagnosis use cases on an application level.
Allocated actor functions	• Provision of door status • Provision of brake status • Provision of input for the Functional Vehicle Adapter
Involved Interfaces	Interface TCMS (ITC)

Table 4 – TCMS System Actor

3.1.1.2 TCMS Data Service

Attribute	Content
Name	TCMS Data Service
Description	TCMS Data Service is an approach to realise TCMS formalisation, the definition and demonstration of methods for a generic TCMS data model and service interface (for communication and control) and for particular use cases, e.g., Doors, Brakes, etc.
Type	External System
Rationale	The integration of the CCS Onboard System into a real train is not foreseen in the demonstrator project due to the nature of a lab demonstrator and absence of an implementing supplier. Nevertheless, the demonstrator evaluates needs and concepts related to migration and train integration. TCMS Data represents means for applications to use information generated in a given TCMS environment, in a uniform way, and not depending on the application itself or its environment.
Allocated actor functions	Adapter Software Component for the formalisation of train specific and provision of generic TCMS data to the SuC

Attribute	Content
Involved Interfaces	Interface Train Adapter (ITA)

Table 5 – TCMS Data Service

3.1.1.3 FRMCS TOBA

Attribute	FRMCS TOBA
Name	The so-called “TOBA box”, is an FRMCS Onboard device integrating FRMCS hardware modems, FRMCS Software as FRMCS Gateway, providing FRMCS interfaces for FRMCS services and transport.
Description	External System
Type	The TOBA box is needed to establish communication between Onboard and Wayside Applications.
Rationale	• Gateway function to FRMCS network • Provision of OBapp Server and MCx clients
Allocated actor functions	Interface FRMCS Onboard (IFO)
Involved Interfaces	FRMCS TOBA

Table 6 – FRMCS TOBA Actor

3.1.1.4 Network Services

Attribute	Content
Name	Network (Management) Services
Description	Services of the Onboard Communication network for communication functionality, network management functionality and CCS/TCMS interoperability.
Type	External System
Rationale	Network Services other that those realised in the SuC will exist in future onboard architectures and should therefore be enumerated here as an external actor.
Allocated actor functions	• Network services to enable virtual network separation, quality of service and prioritisation of data flows on the network • Potentially other network services as DHCP, etc.
Involved Interfaces	Interface Onboard Communication (IOC)

Table 7 – Network Services Actor

3.1.1.5 Date Time Reference

Attribute	Content
Name	Date Time Reference
Description	Date Time Reference is the system/organisation that provides reference of date and time to the SuC. This is an example actor for external shared services.
Type	External System
Rationale	Date and time should be provided by central service. Hence, Date Time Reference has been defined as an actor. Shared Services other than those realised within the SuC will exist in future Onboard Architecture and should therefore be enumerated here as an external actor.
Allocated actor functions	Provide date and time reference to the SuC
Involved Interfaces	Interface Shared Services (ISS)

Table 8 – Date Time Reference Actor

3.1.1.6 Identity and Access Management

Attribute	Content
Name	Identity and Access Management
Description	Identity and Access Management as example for a Security Service that ensures that only assets or entities can access the Onboard Communication Network that are allowed and able to identify themselves. The Security Service summarises relevant technologies and measures to support the secure operation of the demonstrator, e.g., ensuring the authenticity and integrity of the communication between for instance • The SuC and the other on-board units • The SuC and Wayside Assets
Type	External System(s)
Rationale	Security Services other than those realised within the SuC will exist in future onboard architectures and should therefore be enumerated here as an external actor. Provide the Security Layer required by the SuC for operation as the SuC. The SuC may rely on such external services based on results of a security assessment to be performed and supported in the context of WP3.
Allocated actor functions	Provide the Security Layer required by the SuC for operation. • Secured Identity and Access Management

Attribute	Content
	• Public Key Infrastructure (PKI)* • Security monitoring and intrusion (e.g., abnormal network activity) detection* *Only exemplary, assumption is not to realise those functions (might be out of scope for implementation but potentially identified as necessary in a later risk assessment).
Involved Interfaces	Interface Security Services (ISE)

Table 9 – Identity and Access Management Actor

3.1.1.7 Test Environments

Attribute	Content
Name	Test Environments
Description	Test Environment will be set up in the laboratory according to WP36's test strategy, test plans and test cases and in alignment with WP34.
Type	External System
Rationale	In order to conduct testing, extract and collect test results of the demonstration.
Allocated actor functions	Test frameworks for software, potent. static code analyses, coverage, etc. SW in the loop, HW in the loop, open loop testing
Involved Interfaces	Interface Verification and Validation (IVV)

Table 10 – Test Environments Actor

3.1.1.8 ETCS Application Mock-Up

Attribute	Content
Name	ETCS Application Mock-Up
Description	Wayside applications are out of scope but needed as a stimulus for Onboard Demo Applications to be realised in the project. Wayside Applications will be realised in a Mock-up and potentially simulation environment.
Type	External System
Rationale	Wayside Application realised as Mock-Up to serve as a counterpart for Onboard Demo Applications.
Allocated actor functions	Examples: • Mock-Up for provision of Movement Authority • Mock-Up as a control loop
Involved Interfaces	Interface Wayside (IWS)

Table 11 – ETCS Application Mock-Up Actor

3.1.1.9 ATO Application Mock-Up

Attribute	**Content**
Name	ATO Application Mock-Up
Description	Wayside applications are out of scope but needed as a stimulus for Onboard Demo Applications to be realised in the project. Wayside Applications will be realised in a Mock-Up and potentially simulation environment.
Type	External System
Rationale	Wayside Application realised as Mock-Up to serve as a counterpart for Onboard Demo Applications.
Allocated actor functions	Examples: • Mock-Up for Provision of Mission Profile • Mock-Up as a control loop
Involved Interfaces	Interface Wayside (IWS)

Table 12 – ATO Application Mock-Up Actor

3.1.1.10 Digital Register

Attribute	**Content**
Name	Digital Register (Wayside System)
Description	The Digital Register (DR) is an Infrastructure Manager Data System. It acts from the wayside and provides pre-compiled and versioned data sets to the corresponding Onboard Demo Application(s). The current assumption is that a Mock-up will be utilised within the demonstrator setup.
Type	External System
Rationale	The DR wayside system is only needed in case the demonstrator will implement Onboard DR demo application, which is currently uncertain due to the lack of specification and supplier support.
Allocated actor functions	The DR provides input to the SuC and provides input data according to related specifications and processes to be defined in WP27.
Involved Interfaces	Interface Wayside (IWS)

Table 13 – Digital Register Actor

3.1.1.11 Diagnostics Wayside System

Attribute	**Content**
Name	Diagnostics Wayside System

Attribute	Content
Description	The Diagnostics system monitors the state of the SuC and logs parameters of interest. For this purpose, the SuC transmits log, status, and diagnostic data to the Diagnostic system for status evaluation and analysis.
Type	External System
Rationale	Diagnostics system shall cover mainly maintenance topics of an IM in a limited Mock-up realisation within the demonstrator setup. Hence, the diagnostics system has been defined as an actor.
Allocated actor functions	Remote operation of maintenance and servicing functions towards the SuC might be executed via the Diagnostic system.
Involved Interfaces	Interface Wayside (IWS)

Table 14 – Diagnostics Wayside System Actor

3.1.1.12 Maintenance Personal

Attribute	Content
Name	Maintenance Personal
Description	The Maintenance Personal actor is responsible to apply maintenance tasks to the SuC enabling its seamless operation, following relevant operational rules. This actor is an official role in real operation and named here rather for completeness since it is represented (and replaced) by the Laboratory Engineer and System Administrator actors.
Type	Human Actor
Rationale	Actor is mentioned only for completeness.
Allocated actor functions	MDCM functions, everything related to: • Monitoring • Diagnostics • Configuration • Maintenance
Involved Interfaces	Interface Engineering and Maintenance (IEM)

Table 15 – Maintenance Personal Actor

3.1.1.13 Laboratory Engineer

Attribute	**Content**
Name	Laboratory Engineer
Description	The Laboratory Engineer is responsible for many tasks related to the setup, operation, and maintenance of the laboratory.
Type	Human actor
Rationale	Actor is needed for maintaining the implementation in the targeted physical laboratory.
Allocated actor functions	• Diagnose and maintain the SuC's laboratory equipment. • Technical management e.g., detection, processing, and correction of system failure caused by electrical, mechanical, and environmental issues.
Involved Interfaces	Interface Engineering and Maintenance (IEM)

Table 16 – Laboratory Engineer Actor

3.1.1.14 System Administrator

Attribute	**Content**
Name	System Administrator
Description	The System Administrator administrates the demonstrators IT services and environment (SuC and potentially as well a set of external actors) to enable configuration and maintenance activities. The following main actor activities are identified: • Diagnose and maintain the SuC's IT capabilities • Technical management e.g., detection, processing, and correction of system failure caused by the IT infrastructure • System & user administration, e.g., system configuration, assignment of user rights
Type	Human Actor
Rationale	As this is a human actor, it cannot be part of the SuC
Allocated actor functions	The system administrator offers services to the deployed solution for seamless operation and needed maintenance tasks on the setup.
Involved Interfaces	Interface Engineering and Maintenance (IEM)

Table 17 – System Administrator Actor

3.1.2 Interfaces

This chapter defines the interfaces between the SuC and the actors. Each interface is defined by the logical items exchanged between the system and the actor as well as the functional exchanges crossing over this interface. As was mentioned before, the naming of the interfaces is provisional; further development work in subsequent phases is to determine whether existing protocols could be used and whether the interface is constrained by existing standards or not and can therefore be developed according to the needs elicited.

The following figure 4 is based on Figure 2 from chapter 2.4.3.It identifies the system boundary and external interfaces of the SuC.

In comparison to Figure 4, the Train Adapter and Shared Services are partly located inside the SuC since parts of their elements will be realised and integrated into the system.

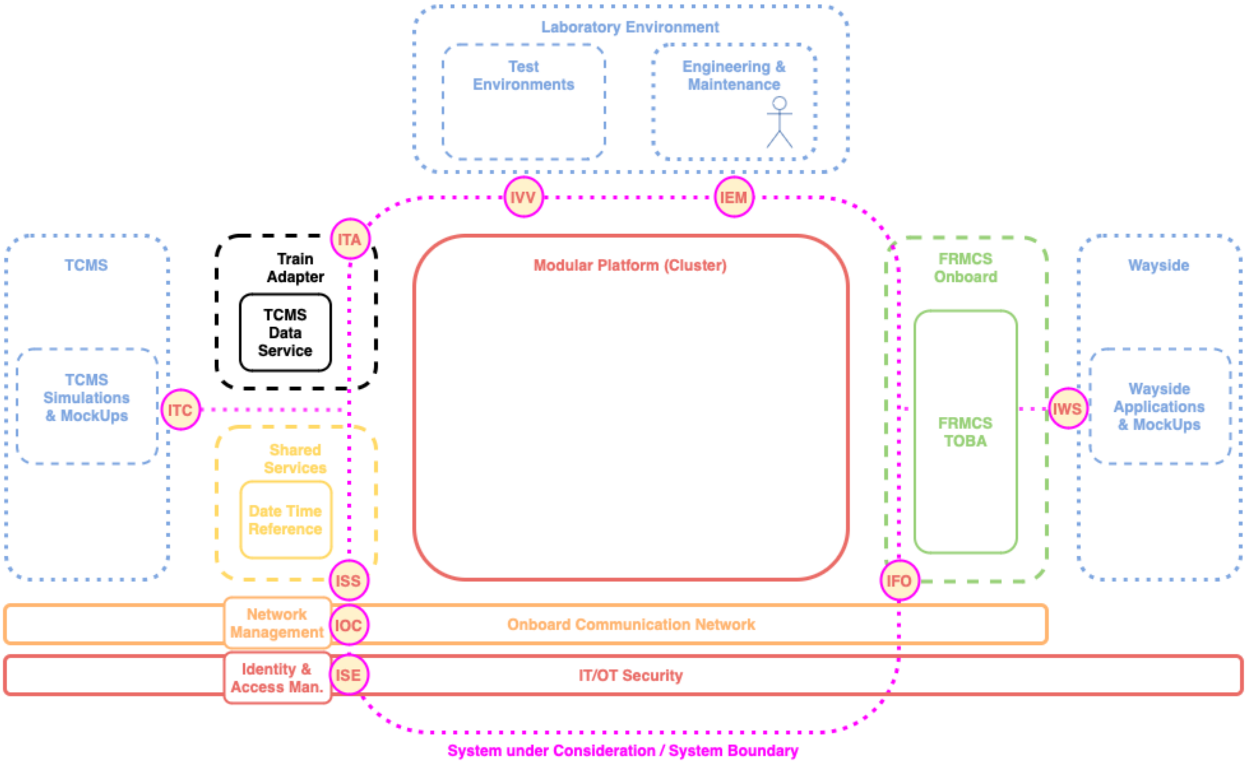

Figure 5 – SuC Boundary and external Interfaces

3.1.2.1 Interface Train Adapter

Attribute	Content
Name	Interface Train Adapter (ITA)
Source	TCMS DataService
Target	Applications hosted on the Modular Platform

Attribute	Content
SUC incoming allocated functional exchanges	Functions (ATO and ETCS) of the CCS Onboard input signals as specified in the TCMS data service [25] • TCMS Data
SUC outgoing allocated functional exchanges	Functions (ATO and ETCS) of the CCS Onboard output signals • CCS Output Data, please refer to OCORA Functional Vehicle Adapter Introduction [21] and related SUBSET specifications mentioned there. • Electrical Signals (not applicable in WP36)

Table 18 – Interface ITA

3.1.2.2 Interface Shared Services

Attribute	Content
Name	Interface Shared Services (ISS)
Source	Time Date Reference
Target	Potentially all relevant Functional Clusters
SUC incoming allocated functional exchanges	The Shared Services consumed by the SuC: • Network Services • Time Service (e.g., from GNSS) • MDCM as remote Diagnostics, Software Update
SUC outgoing allocated functional exchanges	Shared Services Provided by the SuC: • For further Study

Table 19 – Interface ISS

3.1.2.3 Interface Onboard FRMCS

Attribute	Content
Name	Interface Onboard FRMCS (IOF)
Source	FRMCS TOBA Box
Target	CCS Onboard building blocks Applications of other domains as TCMS (out of scop in WP36)

Attribute	Content
SUC incoming allocated functional exchanges	Onboard Application Services (OBapp interface): • Service Stratum of FRMCS • Transport Stratum of FRMCS • Any kind of Application data, incl. Safety and Security protocols
SUC outgoing allocated functional exchanges	Onboard Application Services (OBapp interface): • Transport Stratum of FRMCS • Any kind of Application data, incl. Safety and Security protocols

Table 20 – Interface IOF

3.1.2.4 Interface Onboard Communication

Attribute	Content
Name	Interface Onboard Communication (IOC)
Source	Onboard Communication Network
Target	SuC (and pot. all onboard Cluster)
SUC incoming allocated functional exchanges	All topics specified in UNISIG SUBSET-147 as basis for Onboard Communication**:** • Network Services (e.g., configuration, network management) • Time Service (e.g., from GNSS or other sources) • Network protocols (Layer 1-6) for Separation and Prioritisation (VLAN, QoS, Authentication), Transport, Session, etc. • Any kind of Application data, incl. Safety and Security protocols
SUC outgoing allocated functional exchanges	All topics specified in UNISIG SUBSET-147 as basis for Onboard Communication: • Any kind of Application data, incl. Safety and Security protocols

Table 21 – Interface IOC

3.1.2.5 Interface Security Services

Attribute	Content
Name	Interface Security Services (ISE)
Source	Security Services
Target	Potentially all relevant Functional Cluster

Attribute	Content
SUC incoming allocated functional exchanges	Security Assessment needed: • Signing and/or Encryption of data • Services for Integrity and Authentication and Authorisation
SUC outgoing allocated functional exchanges	Security Assessment needed: • Nothing planned so far

Table 22 – Interface ISE

3.1.2.6 Interface TCMS

Attribute	Content
Name	Interface TCMS (ITC)
Source	TCMS Systems
Target	SuC applications
SUC incoming allocated functional exchanges	TCMS Data as doors, brake states, etc.
SUC outgoing allocated functional exchanges	CCS Data as emergency brake, traction cut of, etc.

Table 23 – Interface ITC

3.1.2.7 Interface Wayside System

Attribute	Content
Name	Interface Wayside Systems (IWS)
Source	Wayside applications
Target	SuC applications
SUC incoming allocated functional exchanges	Wayside application data, e.g., from SUBSET-26
SUC outgoing allocated functional exchanges	CCS application data, e.g., from SUBSET-26

Table 24 – Interface IWS

3.1.2.8 Interface Verification and Validation

Attribute	Content
Name	Interface Verification and Validation (IVV)
Source	Test Environments
Target	SuC systems
SUC incoming allocated functional exchanges	Test plan driven Verification and Validation of the SuC behaviour (to be defined in later phases of the development of the SuC)
SUC outgoing allocated functional exchanges	Behaviour and responses of the SuC

Table 25 – Interface IVV

3.1.2.9 Interface Engineering & Maintenance

Attribute	Content
Name	Interface Engineering & Maintenance (IEM)
Source	System Administrator, Laboratory Engineer
Target	SuC
SUC incoming allocated functional exchanges	• Maintenance or Failure resolution activities (to be defined in later phases of the development of the SuC) • IT configuration data (to be defined in later phases of the development of the SuC)
SUC outgoing allocated functional exchanges	Behaviour and responses of the SuC

Table 26 – Interface IEM

3.2 System Capabilities

The following table introduces a preliminary list of the system capabilities. This list has been derived from the tailoring activities of the SuC's conceptual design and the definition of User Stories during the Task 36.1.

It has been influenced by former activities of the participating partners in initiatives and standardisation activities, their input and experience and by existing specifications (e.g., as reflected in the first two WP26 deliverables and the User Stories & Test Cases document).

This list of system capabilities needs further alignment between the participants of WP36 and depends as well on further input and deliverables of the referenced R2DATO WPs and the System Pillar (as described in chapter 2.3.1).

Since the derived capabilities are not captured in a traceable medium (as Polarion), their assigned numbers might be modified once such changes get performed. While the User Stories defined in the User Stories & Test Cases document are written the perspective "what should be realised by the demonstrator", the system capabilities try to represent the high-level capabilities and functions of the SuC. The table tries to provide a context and rationale for each system capability.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_01	Enable hosting of Onboard Functions up to a SIL 4, mixed SIL, in respect of the targeted TRL of 5/(up to 6) on a Modular Platform.	The Modular Platform implementation in WP 36 shall be able to host mixed SIL applications up to a SIL 4 and target TRL of 5/(up to 6). This implies hardware and software for Onboard usage with the ability to add additional functions without impacting the existing functionality.	The basis platform software has been used in productive systems (safety systems, as inter-lockings and rolling stock safety systems up to SIL 4). Appropriate hardware will be selected, that has already been utilised with this safety software.	Implementation of a Modular Platform, including demo applications (and needed additional software and appropriate hardware) following recommend-dations and specifications of WP 26	None The Modular Platform shall not be impacted by external systems and if so would enter a safe state	The realisation of the Modular Platform concept, including safe and non-safe applications is one of the main objectives in WP 36.
SysC_02	Fulfil typical PRAMSS requirements as well in case of potential hardware failures with focus on safety and security	The Modular Platform is able to enable safe and secure operation of selected demo applications end-to-end, as well in situation when hardware fails.	The platform has been used for wayside safety system (as inter-lockings) and rolling stock safety systems and is certified according to IEC 62443 Security Level 3	A setup of software and hardware components shall be selected and compiled to a system that demonstrates the application of safety concepts as composite fail-safety in line with appropriate security, performance, and redundancy provision.	All external actors End-to-End implies that actors on the wayside and for some use cases as well actors from the TCMS domain are involved, including communication	A system based on Modular Platform and novel communication technologies must realise the same requirements as existing systems. This shall be demonstrated up to the specified TRL.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_03	Fulfil typical PRAMSS requirements in respect to the provision of redundancy	Depending on requirements and setup, all vital functions need to have the possibility to be redundant. Mainly for availability reasons but also for safety reasons, depending on the architecture.	Safety and availability requirements are known and defined	The solution will be realised based on those requirements and can be tested and assessed	Depending on the focus, since redundancy can be applied to different Cluster as Modular Platform, Onboard and FRMCS Communication	At least for the Modular Platform redundancy must be applied, since the safety relies on redundancy in a composite fail-safety approach.
SysC_04	Add application, extend existing on-board solution	Ability to add an application (application using the basic integrity or SIL4 API) to an existing SuC setup in order to verify the possibility to extend the existing SuC with new functionality without impacting the existing functionality.	Full functional SuC that hosts n applications	Full functional SuC that hosts n+1 applications, no impact on the existing functionality.	None if the additional application is self-contained	One objective is to show advantages of Modular Systems as extendibility.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_05	Enable Communication between Onboard Applications, other Onboard Applications and Wayside entities on the Modular Platform	Onboard applications can communicate to wayside (or other onboard realised) applications without knowing the underlying communication technology, or location of the counterpart, the routing of communication end-to-end is handled by the platform and transparent to the hosted application.	Specifications of the concrete wayside entity to communicate with are known (application layer interfaces).	Ability to communicate proven in tests after applying needed configurations (in integration steps).	All, depending on the current application use case(s).	A self-contained application does not fulfil the needs of the system, communication with exchange of data between applications is paramount.
SysC_06	Modular Platform provide sufficient communication, messaging performance in basic integrity or safety context	The system is able to fulfil the communication performance requirements (voting performance, timing, latency, etc.).	Requirements dependant on the application's needs are known. Appropriate measurement controls and abilities are available that ensure uncompromised results.	Proof of performance using some specific tests. Analyse communication flow between different platform native applications (voting performance, timing, latency, etc.), e.g., by using log data, in order to get a feeling about the messaging performance of the Runtime Environment.	Basic tests can be performed on a self-contained system, extending to communication additional actors. May impact. Need to use testing and analysis equipment in the lab environment and human actors may be involved at least for the configuration and the analysis.	Performance requirements get specified by CCS applications. We need to demonstrate that typical performance requirements can be achieved, otherwise, the system would be quite useless. The target TRL raises related measures as well.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_07	Ability to perform Software Updates in a safe and secure way.	Software Updates means to update an application, the configuration of an application (like vehicle parameters, …) and the platform itself.	Provision of new software and configuration. Ability to apply the updates in a safe and secure way.	Updated components are deployed in a safe, secure way and lead to a consistent system with fully achieved integrity.	• Maintenance Personal • Network Services • FRMCS TOBA • Wayside backend • Laboratory Engineer (as provider of artifacts, files, etc.)	Software updates are needed and a key feature of the Modular Platform and shall be demonstrated. In case of remote update, additional actors are involved for transport and on the wayside.
SysC_08	Communicate to “vehicle internal” TCMS systems via the Train Adapter and corresponding interface (ITA)	Communication to internal systems as needed and available to demonstrate the collection and usage of TCMS data in diagnostics use cases.	List of available systems and their data specification. Ability to receive data from the Onboard Communication Network over corresponding protocols, network access, etc.	Proof of communication with a successful test.	• TCMS System • TCMS Data Service • Network Services • DateTime Reference	Demonstration of network access and TCMS data provision is essential for related systems and therefore part of the Grant Agreement.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_09	Ensure safe and secure communication between applications (end-2-end)	Communication between Applications (Onboard-to-Onboard and Onboard-to-Wayside) must be secured by appropriate measures and solutions. This can be achieved on several communication layers and needs further investigation and input, e.g., a security assessment may be conducted.	Requirements provided by WP3 (security), WP 23 for communication solution candidates (ISO OSI Layer 1-6) and for FRMCS (please refer to chapter 2.3.1). Assumptions may be made in respect and potential protection demands of applications.	Appropriate safety and security protocols and controls are identified and partly realised for explicit use cases.	• FRMCS TOBA • Network services • DateTime Reference • Identity and access management	Safety and Security must be applied end-to-end.
SysC_10	Ensure secure operation in case a security threat gets initiated	Apply security controls based on a security assessment and realise appropriate measures and controls for a secure operation of the SuC.	Security requirements are known, and security threat can be detected. This may not be based on intrusion detection but rather on the knowledge of a security vulnerability. Denial of service attacks could be detected more easily.	Appropriate action have been defined and can be applied.	• FRMCS TOBA • Network services • Identity and Access Management	Secure operation is mandatory in future operation.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_11	Collect, aggregate, and provide Diagnostic data from onboard applications to the trackside	Diagnostic data from Onboard applications shall be collected and provided to a wayside diagnostic backend in a unified and harmonised way, e.g., for health and performance monitoring, logging, configuration and maintenance purpose.	Diagnostics data can't be collected and aggregated in a harmonised way and is not accessible from remote or even only to specialists or suppliers in proprietary formats	A unified, harmonised and centralised approach got realised	• Diagnostics Wayside Systems • FRMCS TOBA • Network Services • TCMS system • TCMS Data Service	Novel harmonised approach for Onboard Diagnostics shall be evaluated according to Grant Agreement.
SysC_12	Onboard demo applications performing control loops end-to-end to the wayside	Applications dedicated for up to SIL4 (e.g., ETCS) and basic integrity (e.g., ATO) will make use of services and abilities of the Modular Platform to showcase safe and secure hosting, communication and the utilisation of Diagnostics functions.	Onboard applications can only be realised by integrating complete solutions (mainly monolithic systems, bundeling a set of functions, including software and hardware)	Onboard applications can be tendered separately, integrated and potentially be reused on Modular Platforms from different suppliers for both, applications and platform.	• FRMCS TOBA • ETCS and ATO wayside Mock-Ups • Network Services • Date Time Reference • Identity and access management	The idea is to showcase Onboard realisations with stimulus from wayside.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_13	Train Integration Concepts get applied and evaluated and train data gets used in a harmonised way	Integration into existing trains is supported by train adapter concepts, that will be partly realised in a context of TCMS simulations and deliverables from WP 31	Train Integration is performed for each train series and type separately, which cases high cost	The integration of a standardised future CCS Onboard platform gets supported and facilitated by solutions that enable harmonised interfaces and reduce complexity	• TCMS system • TCMS Data Service	The roll-out of ETCS needs solutions that enable a cost effective and manageable integration of future CCS Onboard systems into existing trains
SysC_14	Ensure application communication via FRMCS communication path	FRMCS controlled communication path shall be used to perform communication between onboard application endpoint and wayside application endpoints	Applications are connected to FRMCS onboard and wayside	Proof of communication via FRMCS controlled communication path	• FRMCS TOBA Wayside actors as • ETCS Application Mock-Up • ATO Application Mock-Up • Digital Register • Diagnostics Wayside System	Ensure usage of FRMCS communication and not bypassing it.

ID	System Capability	Description	Pre-condition	Post-condition	Involved actors and ext. systems	Rationale
SysC_15	Onboard application connected via FRMCS standardized interfaces	Connection between Onboard application and FRMCS onboard shall use standardized FRMCS interface OBapp	IP connectivity between Onboard application control and FRMCS onboard is available	FRMCS onboard is connected via OBapp interface to Onboard controller	FRMCS TOBA	Ensure usage of standardized FRMCS application connection interface OBapp and test interface feasibility.
SysC_16	FRMCS Onboard is integrated in Onboard modular architecture	FRMCS Onboard components shall be integrated into the modular onboard architecture and to the Onboard communication Network and utilizing the relevant associated communication interface to communicate to the onboard applications	SW and interface integration requirements defined	FRMCS onboard components integration in onboard architecture	FRMCS TOBA	Ensure feasibility of integration of FRMCS onboard components in on-board architecture

Table 27 – Collection of System Capabilities of the SuC

4 OPERATIONAL CONDITIONS

4.1 SCOPE OF OPERATIONAL REQUIREMENTS INFLUENCING THE SYSTEM

4.1.1 System operating conditions and constraints

Operating conditions and constrains will be worked out during the implementation tasks based on the implementation plan for virtual and physical laboratory implementations. As described in the SoW the demonstrator setups will comprehend virtual environments (manly used in the beginning) and finally physical lab implementations plus additional infrastructure (e.g., for FRMCS, configuration management, continuous integration, and deployment). Corresponding concepts will be defined in the later implementation tasks of the project.

4.1.2 System maintenance conditions

IT access and deployment strategies (e.g., for the development and continuous integration based on reliable automatic configuration and test procedures) will be worked out and conducted in the later implementation tasks of the project.

4.1.3 Human Interaction

As the SuC is focused on prototyping and testing, further human interaction in addition to the System Administration and Laboratory Engineering is not expected. A preliminary Identification of human interaction would include test infrastructure required by testing staff, e.g., test interfaces, additional data capture needs etc. They are to be worked out in later stages in the lifecycle of the project and reflected in the respective documentation (e.g., IVV strategy [16]). A chapter for testing and a first set of corresponding test cases has been added to the document User Stories & Test Cases.

In order to implement and use the SuC, training as well as operating manuals have to be provided. Related activities and responsibilities are part of the SoW and its implementation plan.

4.1.4 Interactions with other personnel and public

As the operation of the SuC is envisaged to be performed within a non-public laboratory, no further interactions are expected. There is no influence to be expected on employees (e.g., maintenance personnel) and public.

In order to implement and use the SuC, training as well as operating manuals have to be provided. Related activities and responsibilities are part of the SoW and its implementation plan.

4.1.5 Operating Procedures and Modes of Operation

The following main modes of operation are covered by the system:

- Normal operation
- Degraded operation (system with limited functionality, only partly covered)
- Maintenance operation
- Diagnosis operation

Several use cases that would be part of a system in a productive operation will not be handled by the SuC. Degraded situations, recovery procedures to normal operation or loss and recovery of integrity may be evaluated by the SuC in some use cases.

The definition of the exact operational procedures is out of scope.

4.2 Risk Analyses/Assumptions

4.2.1 Scope of the Risk Analysis

A Risk Analysis has to encompass all elements of a system to gain an understanding of the safety ramifications in the introduction of a novel system. The safety approach shall be incorporated and ensured by the system design as both Human and Organisational Factors need to be considered through following a risk-based approach to delimitate safety rules and measures. The deliverables of WP8 [16] may provide guidance here but a future risk analysis is not foreseen in WP36.

4.2.2 Assumption on the Safety Classification

The safety classification for the SuC would be subject to a subsequent safety analysis to be performed. Due to the nature of a demonstrator project such activities are not foreseen. The current assumption is that the SuC shall support mixed criticality up to a SIL4. Certification and homologation aspects shall be evaluated in WP26 [12].

5 OPEN POINTS

Number	Description	Comments	Status
ToDo01	Refinement of system capabilities	The system capabilities may be influenced by respective deliverables of the R2DATO program named in [6] to [16].	open
ToDo02	Brake-down of functions allocated to the system for the defined particular interfaces.	Based on the system capabilities a list of functions to be performed by the SuC will be identified and described. It can be a preliminary list of functions and/or a preliminary system requirements specification depending on the level of application and on the level of known details of the functions.	open
ToDo03	The functional exchanges between these functions allocated to those particular interfaces.		open
ToDo04	Define the functional exchanges between functions allocated to interfaces.		open
ToDo05	Operational conditions and constraints for the development, laboratory environments and validation		open

Table 28 – Open Points

6 CONCLUSIONS

This “System Definition” document is part of the “Demonstrator Specification”, the first deliverable D36.1 of the R2DATO Onboard Platform Demonstrator work package. The purpose of a system definition document is to set the technical scope and purpose of the intended system, defining its purpose, environment, system boundary, system capabilities, system functions and interfaces.

The identification of relevant input sources, dependencies, the definition of needed assumptions and restrictions followed by a structured approach specifying the SuC’s conceptual shall set the basis for further analysis, architectural work on both, system, and sub-system level.

The intention is to manifest the demonstrator’s specification as a basis for further design and realisation to enable the fulfilment of the objectives defined in the Grant Agreement the SoW and User Stories of WP36.

This System Description document provides the needed black-box view on system level to the Architecture document and realises a comprehensive und reliable basis for future Implementation Tasks 36.2 - 36.4.

While most of the intended goals have been achieved, further brake-down and refinement is needed as pointed out in the chapter 5 Open Points. The next important steps have already been initiated and many knowns are covered in the corresponding additional documents of this deliverable, the User Stories & Test Cases and Architecture documents. Next to those technical specifications it is on equal significance that the project partners have gained a common understanding, and that commitment exists on the planning and proposed realisation in the upcoming implementation tasks.

The whole endeavour still holds back many challenges and pitfalls but from the expectations towards a system definition hopefully get met with this first technical document.

REFERENCES

[1] R2DATO Onboard Platform Demonstrator Specification

[2] R2DATO Onboard Platform Demonstrator Statement of Work

[3] R2DATO Onboard Platform Demonstrator User Stories & Test Cases

[4] R2DATO Onboard Platform Demonstrator Architecture

[5] ERJU IP GRANT AGREEMENT Project 101102001 - FP2 - R2DATO, 2022

[6] R2DATO D23.2 - Definitive and aligned requirements set for Onboard Communication Network

[7] R2DATO D23.3 - List of solution candidates, publication planned December 2023

[8] R2DATO D23.4 - Proposal on TSI202x, SS-147, publication planned July 2024

[9] R2DATO D26.1 - High-level consolidation of prior work and agreement on the Modular Platform specification

[10] R2DATO D26.2 - Intermediate Modular Platform requirements, architecture and specification

[11] R2DATO D26.3 - Final Modular Platform requirements, architecture and specification, publication planned October 2024

[12] R2DATO D26.4 - Summary of findings and recommendations from study on modular certification and homologation, publication planned October 2025

[13] R2DATO D27.2 - Specification of the Digital Register implementation(s) required in FP2-R2DATO, publication planned November 2023

[14] R2DATO D27.6 - Documentation of the implementation of the Interaction between Trackside and Onboard, due November 2025

[15] R2DATO D31.3 - Demonstrator: TCMS Formalisation: TCMS formalisation, Prototypical implementation (TRL 4-5) of a TCMS Data Service

[16] R2DATO Onboard Platform Demonstrator IVV, derived from WP 34, 35

[17] R2DATO WP8 - Safety Analysis & Risk Assessment

[18] RCA Baseline 1 Release 0, 2022

[19] Shift2Rail https://projects.shift2rail.org

[20] OCORA-CCS On-Board Architecture https://github.com/OCORA-Public/Publications/tree/master/00_OCORA Latest Publications/Latest Release

[21] OCORA CCS On-Board Functional Vehicle Adapter Introduction

[22] European Union TRL Definitions (https://euraxess.ec.europa.eu/career-development/researchers/manual-scientific-entrepreneurship/major-steps/trl)

[23] CENELEC The European Committee for Standardization

[24] TSI 2023 - https://www.era.europa.eu/domains/technical-specifications-interoperability_en

[25] Eurospec TCMS data service https://eurospec.eu/tcms-data-service/

ANNEX A: TRACING CONCEPT

This Annex illustrates tracing concepts that may be considered to facilitate the flow of information. The concept illustrated in Figure 6 illustrates a function-based tracing, while the concept in Figure 7 may become applicable as a further step based on the availability of a comprehensive set of system requirements.

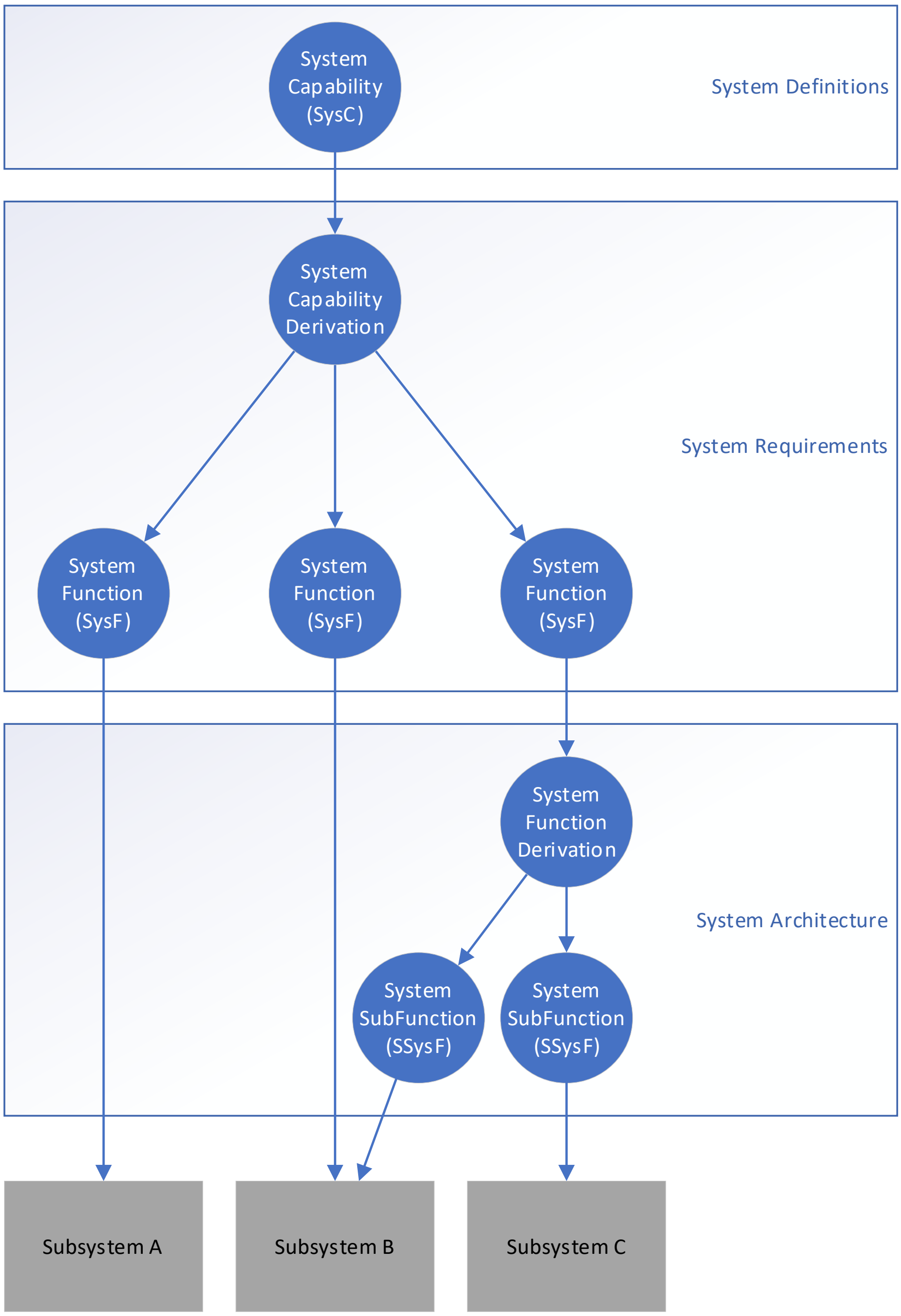

Figure 6 – Function based tracing

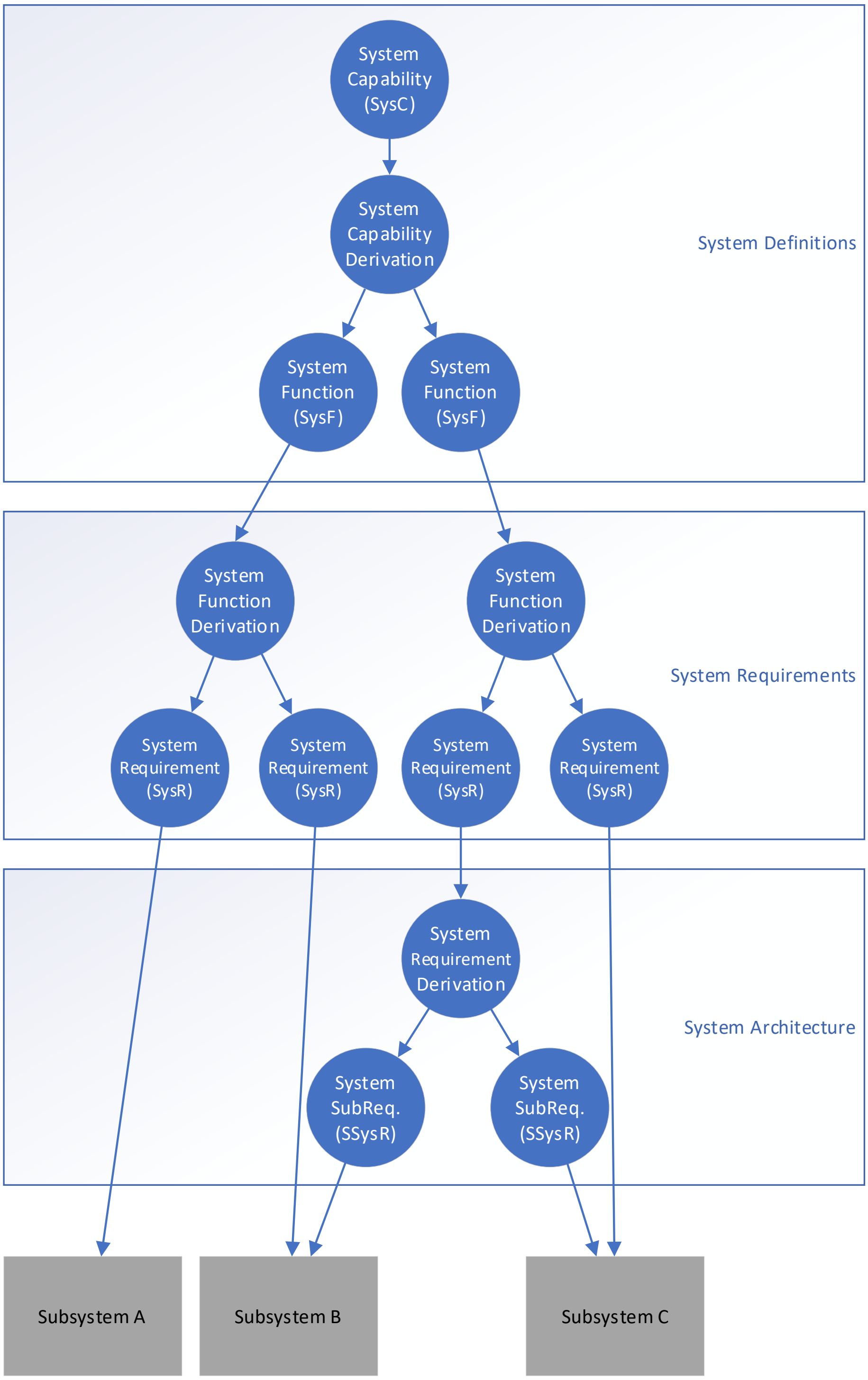

Figure 7 – Requirement based tracing