Rail to Digital Automated up to Autonomous Train Operation

D36.1 – Demonstrator Specification

Statement of Work

Leader/Responsible of this Deliverable: DB

Reviewed: Y

Document status		
Revision	Date	Description
0	11/09/2023	Initial version
1	12/10/2023	Refined version with input from all partners
2	19/10/2023	Refined version after internal review
3	25/10/2023	Version for TMT review
4	30/11/2023	Unchanged version (only footer update)

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	

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

ACKNOWLEDGEMENT

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.

Disclaimer

TABLE OF CONTENTS

Acknowledgement ... 2
Table of Contents ... 3
Table of Figures ... 4
1 Introduction ... 5
1.1 Background ... 5
1.2 Purpose of this Document ... 5
1.3 Scope ... 5
1.4 Objectives ... 6
2 Tasks ... 6
2.1 Consolidation of existing specifications and derivation of demonstrator specification ... 7
2.2 Demonstrator Implementation and Testing Phase 1 ... 7
2.3 Demonstrator Implementation and Testing Phase 2 ... 7
2.4 Demonstrator Implementation and Testing Phase 3 ... 8
2.5 Analysis of Setup and Preparation of Blueprint for EU-RAIL Phase 2 and Beyond ... 8
3 Implementation Plans ... 8
3.1 Project Infrastructure ... 8
3.1.1 Configuration Management ... 9
3.1.2 Virtual Lab Environment ... 10
3.1.3 Physical Lab Environment ... 11
3.2 Modular Computing Platform ... 12
3.2.1 Safety Layer / Runtime Environment (RTE) ... 12
3.2.2 FRMCS Platform Functions ... 13
3.3 Shared Services ... 14
3.3.1 Monitoring, Diagnostics, Configuration and Maintenance (MDCM) ... 14
3.4 Test Environment ... 16
3.4.1 Onboard Communication Network ... 16
3.4.2 FRMCS TOBA & Trackside Entity ... 17
3.4.3 Train Adapter / TCMS Data Service ... 18
3.4.4 IT/OT Security ... 19
3.5 Demo Applications ... 19
3.5.1 ATO Control Loop ... 20
3.5.2 ETCS Control Loop ... 21
3.5.3 Digital Register ... 21
4 Verification and Validation ... 22
5 Collaboration ... 23

TABLE OF FIGURES

Figure 1: Demonstrator Setup 6
Figure 2: Diagram of the Process Model.. 23

1 INTRODUCTION

1.1 BACKGROUND

In the work package 36 (WP36) “Onboard Platform Demonstrator” the partners Deutsche Bahn (DB), Ground Transportation Systems (GTS), Kontron (KONTRON), Schweizerische Bundesbahnen (SBB), Siemens Mobility (SMO) and Trafikverket (TRV) cooperate to validate the feasibility of a future-proof onboard IT-platform that is suitable to host safety critical applications.

In the context of R2DATO this work package demonstrates a concrete implementation of the modular computing platform based on the available input from work package 26 to a Technology Readiness Level (TRL) 5/6 (demonstrated in relevant environment) enhanced by onboard connectivity to a train adapter, FRMCS communication modules and shared services (e.g., diagnostics and maintenance).

The project timeline started in December 2022 (M1) and ends in May 2026 (M42).

1.2 PURPOSE OF THIS DOCUMENT

The Statement of Work (SoW) refines the work package description of the grant agreement to a commitment of the work to be done. It especially details the objectives, scope and aspects that are written as conditionals in the grant agreement.

Among the partners it serves as an agreement on the exact work split and provides an implementation plan for the demonstrator setup and execution.

1.3 SCOPE

The onboard modular computing platform (from hardware to application integration) is the main object of demonstration of this work package up to TRL 6. Key aspects are a hardware abstracted safety layer (runtime environment to host applications up to Safety Integrity Level 4), that provides a standardised API towards the applications (as far as defined by work package 26), and functions for safe communication among applications. It is also demonstrated that the modular computing platform allows for mixed criticality workloads on the same hardware.

The System under Consideration (SuC) is the Modular Computing Platform integrated into its relevant environment. It interfaces to an onboard communication network with a train adapter, shared services, an FRMCS onboard system and measures for IT/OT security. Not being the main object of demonstration, the latter systems are implemented up to TRL 5.

Even though the aim of the modular computing platform is to host several different applications on one instance, a train consist may embody multiple instances of the modular computing platform. As an enabler for modular Onboard Control-Command and Signalling (CCS) Systems beyond one instance of the modular computing platform a standardised Onboard Communication Network is a vital environment.

Next to basic network functions, the shared services include diagnostics parts of Monitoring, Diagnostics, Configuration and Maintenance (MDCM). There are no railway standards available that define interfaces for onboard diagnostics and software / configuration changes. This work package relies on existing solutions to demonstrate technical feasibility by one possible implementation. The safety related process of updating onboard systems is not in focus and will not be considered.

Beyond the system under consideration the demonstrator setup also includes a wireless communication to a trackside entity via FRMCS as well as simulated data sources / sinks to execute and visualize the test scenarios in a presentable way.

Main driver of the demonstration are demo applications that are used to showcase specific capabilities of the modular computing platform. They are implemented as application dummies with only minimal functional scope.

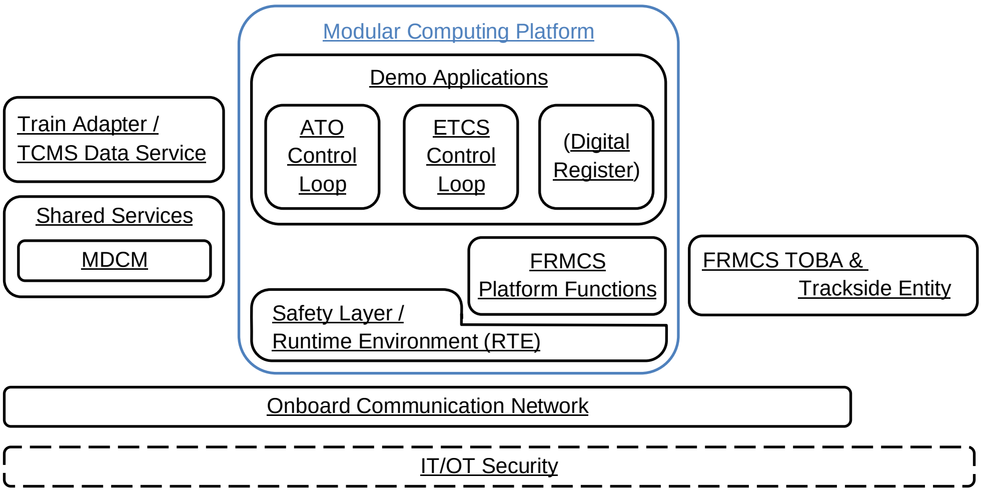

Figure 1: Demonstrator Setup

1.4 Objectives

By implementing a demonstrator of the modular computing platform as a physical lab setup in a relevant environment, this work package provides a high-level blueprint of the core concepts for future onboard modular computing platform demonstrations (e.g., for EU-RAIL phase 2), giving a technical recommendation on the appropriate level of modularity.

It delivers comprehensive findings on the feasibility of the implementation and integration of safety critical and mixed criticality applications on such a modular computing platform and identifies existing gaps in specifications and available solutions. Where possible, it also provides suggestions how to fill such gaps based on the learnings from the demonstration.

2 TASKS

The work package is structured in five tasks, the second to fourth of which are implementation tasks that focus on different topics and realize different parts of the demonstrator. Each task is headed by one of the partners who is responsible to coordinate the work in the task and, on completion of the task, hands over the demonstrator implementation to the next task leader.

All participating partners actively contribute to the tasks and fulfil their commitments to respective topics as stated in the Implementation Plans. In this regard, the task objectives outline the joint commitment of all participating partners on the status of the demonstrator implementation at the end of each task.

2.1 CONSOLIDATION OF EXISTING SPECIFICATIONS AND DERIVATION OF DEMONSTRATOR SPECIFICATION

Number: 36.1

Duration: M1 to M12 (Dec 2022 to Nov 2023)

Leader: DB; Participants: SMO, GTS, KONTRON, SBB, TRV

In this task the partners agree on the specific demonstrator setup including the system definition, this statement of work with the implementation plan, the user stories and test cases for the demonstrator as well as the envisioned demonstrator system architecture.

2.2 DEMONSTRATOR IMPLEMENTATION AND TESTING PHASE 1

Number: 36.2

Duration: M10 to M20 (Sep 2023 to Jul 2024)

Leader: GTS; Participants: SMO, DB, KONTRON, SBB

For the MVP 1, the modular computing platform is first deployed in a virtual environment together with demo application dummies of different safety levels, that allow to test the communication between safety critical applications as well as mixed criticality applications.

While no specific safe communication protocol is implemented, the support for the possible integration of such protocols is also investigated.

The setup in the virtual lab environment aims to resemble the later physical deployment already closely to test hardware, network and application configuration needed to run the modular computing platform in its relevant environment. This also enables virtualised and parallel integration testing.

A transfer to a physical lab environment starts already during this task to enable an early integration of all systems (walking skeleton).

2.3 DEMONSTRATOR IMPLEMENTATION AND TESTING PHASE 2

Number: 36.3

Duration: M21 to M30 (Aug 2024 to May 2025)

Leader: KONTRON; Participants: SMO, GTS, DB, SBB

The MVP 2 extends the demonstrator setup from the virtual lab environment to a physical lab environment and enhances the functional scope by train integration services, diagnostics functions and FRMCS communication.

The FRMCS TOBA hardware is integrated over the common onboard network with reference implementation dummy applications of different safety levels on the modular platform.

A theoretical study also investigates to which extent the TOBA solution could be modularised, running parts of the software on the modular computing platform, e.g., utilizing OB_{rad} to communicate directly from the modular computing platform to the modem(s).

Vehicle diagnostics services are deployed on the modular computing platform and connected with a train integration service over the common onboard network.

2.4 Demonstrator Implementation and Testing Phase 3

Number: 36.4

Duration: M25 to M40 (Dec 2024 to Mar 2026)

Leader SBB; Participants: SMO, GTS, KONTRON, DB

In the final demonstrator setup, the simplified demo onboard applications are integrated on the modular computing platform together with mockups of respective trackside application counterparts communicating over FRMCS.

To the extent possible within the work package, the physical common onboard network (CCN) is adapted to the latest specification of UNISIG SUBSET-147.

The Monitoring, Diagnostics, Configuration and Maintenance services (provided by DB as described in the Implementation Plan) are integrated with the safety layer / runtime environment over a standardised diagnostics interface.

2.5 Analysis of Setup and Preparation of Blueprint for EU-RAIL Phase 2 and Beyond

Number: 36.5

Duration: M36 to M42 (Nov 2025 to May 2026)

Leader: DB; Participants: SMO, GTS, KONTRON, SBB, TRV

In the last task, the findings from the demonstrator implementation are consolidated and transformed into a recommendation of an onboard modular computing platform concept blueprint that can serve as basis for integrated demonstrators in EU-RAIL phase 2.

3 IMPLEMENTATION PLANS

This section details the implementation plans for different areas of the demonstrator that generally contribute to multiple tasks of the work package. For each area, one of the partners takes the overall responsibility to do and/or facilitate what is required to provide the expected results over the whole runtime of the work package (until May 2026 / M42). In the special case of a "shared" responsibility for one area, the responsibility is stated for each work item individually.

3.1 Project Infrastructure

To conduct the work of this work package, some basic infrastructure is needed in addition to what is provided to the R2DATO project in general.

Additional capabilities that are expected from the partners individually to execute the work items they provide to the work package (e.g., for individual procurement or software development) are not named in this section.

3.1.1 Configuration Management

→ Overall responsibility: DB

→ Objectives:

- Organize and trace working products in relation to the user stories, test cases and test results of the work package.
- Provide a single source of truth for all source code, configuration, and further software artefacts, necessary to execute the demonstrator to ensure reproducibility of test results.
- Enable CI/CD workflows for the demonstrator setup.

→ Preconditions:

- All partners can provide a Microsoft business account for all colleagues who contribute source code, configuration, or other software artefacts to the work package.
- A containerised integration pipeline for the Safety Layer / Runtime Environment (RTE) is provided by GTS.
- Internet access of Physical Lab Environment and local computing resources to host the CD runner.

→ Work items:

Q1/2024 / M14: Tool / Process Setup

- Setup of a central (Git) repository.
- Definition of configuration management processes.
- Provision of repository access to the project partners (up to three colleagues each).

Q2/2024 / M17: Continuous Integration (CI)

- Setup of a continuous integration pipeline for functional applications on the TAS Platform in cooperation with GTS.

Q3/2024 / M20: Continuous Deployment (CD)

- Setup of a continuous deployment pipeline for the demonstrator setup to the physical lab target in cooperation with the SBB.

Q2/2026 / M42: Aftercare

- Archive data and close the central repository.

→ Results:

- M14: Central repository for source code, configuration, and further software artefacts.
- M15: Documentation of configuration management process.

3.1.2 Virtual Lab Environment

→ Overall responsibility: GTS

→ Objectives:

- Provide virtual environment with TAS Platform development toolchain and deployment targets
  - on local machines.
  - on local training server (virtual machines accessed by VNC in local network at the TAS Platform training).
  - on central server (virtual machines accessed by VNC).

→ Preconditions:

- TAS Platform development training is conducted by GTS.
- Development toolchain and virtual deployment targets are provided as containers by GTS.
- Agreement on modalities of central virtual lab is documented (how to work).
- Central UNIX-server with container runtime is provided (by SBB as part of the Physical Lab Environment, later also used as server for the Shared Services).
- Basic specification of the Onboard Communication Network is available.

→ Work items:

Q4/2023 / M12:

- Setup of containerised development toolchain and deployment targets for the TAS Platform training on a GTS owned device that can be locally accessed during the TAS Platform training.

Q1/2024 / M16:

- Enable the SBB for the setup of the containerised TAS Platform development toolchain and virtual deployment targets on a central server.
- Enable the setup and configuration of additional virtual machines for remaining onboard components (e.g., Shared Services, Train Adapter / TCMS Data Service, Safe I/O) and a virtual onboard network (e.g., configuring VLANs).

→ Results:

- M12: Availability of virtual lab environment to host TAS Platform development toolchain and virtual deployment targets during the TAS Platform training.
- M16: Availability of virtual lab environment with TAS Platform development toolchain and virtual deployment targets for continuous use.
- M16: Configuration for virtual (integration) test environment (without FRMCS TOBA & Trackside Entity) and deployment on a central server.

3.1.3 Physical Lab Environment

→ Overall responsibility: SBB

→ Objectives:

- Demonstrate integration with real onboard suitable hardware to test the modular computing platform up to a technology readiness level 6 (demonstrated in relevant environment).
- Derive a presentable demonstrator showcase.
- Test physical hardware failure scenarios.

→ Preconditions:

- Availability of
  - Specification of server for Virtual Lab Environment as well as documentation for the setup of the containerised TAS Platform development toolchain and virtual deployment targets provided by GTS
  - TAS Platform suitable hardware as 2oo3-system (including safe I/O)
  - FRMCS (TOBA) box hardware
  - Onboard communication network (configured switches)
- Work package 36 partners continuously support their provided hard- and software.

→ Work items:

Q4/2023 / M13: Setup Server Infrastructure for Virtual Lab Environment

- Order and setup of Shared Services server based on specification of GTS provided at the TAS Platform training.
- Installation of the containerised TAS Platform development toolchain as well as a virtual deployment target as VMs on the Shared Services server based on documentation provided by GTS.

Q1/2024 / M14-M18: Preparation of Demonstrator Setup

- Prepare and clean lab location.
- Draft complete list of needed hardware components (router, server, service laptop and other hardware compliant with UNISIG SUBSET-147).
- Source and order the needed hardware.
- Organize internet gateway / firewall and access for external contributors.
- Setup connection to Kontron labs (A and F).

Q3/2024 / M21-M30: Initial Lab Build-up

- Coordination with work package 36 partners (SMO, GTS, DB, KONTRON) to integrate Safety Layer / Runtime Environment (RTE) (TAS Platform), Monitoring, Diagnostics, Configuration and Maintenance (MDCM), Onboard Communication Network, FRMCS TOBA & Trackside Entity,

Q2/2025 / M31-M40: Ongoing Operation and Maintenance of the Physical Lab

→ Results:

- M27: A physical lab setup to host the Modular Computing Platform and Shared Services as well as the Test Environment and serving as integration platform for all work package 36 Demo Applications; including:
    - Modular computing platform 2oo3-custer
    - Server resource for Shared Services
    - Server resource for Train Adapter / TCMS Data Service
    - Trackside WIFI access point
    - Server resource for trackside gateway including environment for VM deployment
    - Connection to Kontron labs (A and F)
- M27: A physical Onboard Communication Network adhering to UNISIG SUBSET-147 in its latest available version.
- M30: Remote access to monitor and administer the physical lab setup.

3.2 Modular Computing Platform

The modular computing platform is the main object of demonstration in the work package. It consists of the hardware, operating system, middleware, and runtime environment as well as necessary services and communication gates to execute workloads up to SIL 4 that can communicate with other entities on the modular computing platform and connected via the Onboard Communication Network.

Next to the Safety Layer / Runtime Environment (RTE), the FRMCS Platform Functions allow to establish FRMCS connections that can be used by applications of different safety levels on the modular computing platform.

3.2.1 Safety Layer / Runtime Environment (RTE)

→ Overall responsibility: GTS

→ Objectives:

- Project partners understand the programming model on the RTE (TAS Platform) as it is provided by GTS.
- Minimal safe application dummy ("ping-pong") is available as reference implementation for further Demo Applications.
- Test basic platform user stories in a minimal setup available after the TAS Platform development training.

→ Preconditions:

- Availability of a server to host a Virtual Lab Environment by Q4/2023.
- Availability of hardware to host the modular computing platform in the Physical Lab Environment by Q2/2025.

→ Work items:

Q4/2023 / M12:

- Conducting two-day development training based on TAS platform from GTS for up to 10 participants.
- Deployment of TAS platform and minimal safe application dummy in Virtual Lab Environment.

Q1/2024 / M14:

- Test of basic platform user stories (e.g., deployment configurations, communication between safe and mixed criticality applications) on Virtual Lab Environment.
- Further support on usage of demo application from TAS Platform development training by consideration of topics such as communication, redundancy, safety, diagnostics.

Q2/2024 / M16 to Q2/2026 / M42:

- Support for service and application integration on Modular Computing Platform in Virtual Lab Environment and Physical Lab Environment.
- Provision of recent product updates to the TAS Platform.

Q3/2024 / M21:

- Deployment of TAS platform and minimal safe application dummy on Physical Lab Environment

Q3/2025 / M33:

- Integration of software update functions for configuration, applications, and operating system.

→ Results:

- M13: TAS Platform development training
- M13: Reference implementation for communication path from Model 1 task set over Model 3 task set (communication gate) to network application (“ping-pong” dummy application)
- M16: TAS Platform deployed on Virtual Lab Environment
- M16: Test and validation of basic modular computing platform user stories
- M22: TAS Platform deployed on Physical Lab Environment
- M34: Example for software update workflow (based on available abilities of the used platform solutions, leaving the specification to other domains)

3.2.2 FRMCS Platform Functions

→ Overall responsibility: Shared

→ Objectives:

- Demonstrate abstraction of FRMCS communication (transparent to the application) on the modular computing platform as reusable component.

→ Preconditions:

- TAS Platform development training by M20
- FRMCS TOBA & Trackside Entity for E2E testing by M27

→ Work items:

Q3/2024 / M21:

- Kontron: Development of a static configured OBapp client reference implementation as basic integrity application (preferred on POSIX).
- Kontron in collaboration with GTS: Development of the OBapp client gate (Model 3 task set on TAS Platform).

- Kontron: Documentation of reference implementation / configuration of end2end FRMCS communication loop (e.g., "ping-pong" dummy application from TAS Platform training via FRMCS) and consulting for partners.

Q1/2025 / M27:

- Kontron: Definition of test plan for FRMCS end2end communication test.
- Kontron: Execution of end2end test of FRMCS functions.

→ Results:

- M16: OBapp agent (super loose) concept available
- M24: OBapp gate on Modular Computing Platform (loose coupling)
- M28: OBapp agent (super loose) implementation available
- M30: Successful reference implementation / test execution of end2end FRMCS communication loop.

3.3 Shared Services

The shared services include a broad range of basic integrity functions that are reusable over the whole onboard domain. The Monitoring, Diagnostics, Configuration and Maintenance (MDCM) services are part of the system under consideration of this work package. Additional shared services are provided to the demonstrator setup as test environment in the context of the Onboard Communication Network.

3.3.1 Monitoring, Diagnostics, Configuration and Maintenance (MDCM)

→ Overall responsibility: DB

→ Objectives:

- Demonstrate vehicle abstraction for vehicle diagnostics data.
- Demonstrate diagnostics interfaces for vehicle data, application business logic and platform runtime monitoring.
- Demonstrate FRMCS communication on Modular Computing Platform without dependency to the Safety Layer / Runtime Environment (RTE) (diagnostics functions as basic integrity applications).
- Demonstrate mixed-criticality setup on one Modular Computing Platform.
- Demonstrate possible software update workflows.

→ Preconditions:

- TAS Platform development training by Q1/2024.
- Reference implementation for communication path from Model 1 task set over Model 3 task set (communication gate) to network application in Q1/2024.
- Virtual Lab Environment available by Q2/2024.
- Physical Lab Environment including "service laptop" equipment available by Q1/2025.
- TCMS Data Service as-is available by Q1/2024 and final implementation for demonstrator by Q2/2025
    - Possibility to adapt the TCMS Data Service to the Onboard Communication Network according to UNISIG SUBSET-147
- OBapp agent concept by Q1/2024 & implementation by Q1/2025 from FRMCS Platform Functions

→ Work Items:

Q3/2023 / M10: DIA System and Software Architecture

- Definition of diagnostics modules, their interfaces, main functions and mapping to demonstrator user stories.

Q4/2023 / M12: Procurement Preparation

- Statement of Work for an MDCM solution to engage in a research and development partnership with an external supplier.

Q1/2024 / M16: Provision of Simulation, TCMS Data Service (existing version) and DIA-VEC Agent

- Integration of the simulation & TCMS Data Service on Virtual Lab Environment.
- Provision of DIA-VEC Agent (generated C-Code from Project BaseDev 1.0 + 2.0 for POSIX environments) and integration as basic integrity application next to the Safety Layer / Runtime Environment (RTE) (mixed-criticality).
- Concept for communication methods (user stories for DIA-VEC)
    - DIA-VEC → basic integrity application on safety layer (TAS Platform Model 3 task set)
    - DIA-VEC → safe application (TAS Platform Model 1 task set) on safety layer via communication gate (TAS Platform Model 3 task set with message queue adaption)
    - DIA-VEC → wayside via OBapp agent
    - DIA-VEC → "service laptop" attached to the Onboard Communication Network

Q2/2024 / M19: Integration of DIA-VEC Agent with Safety Layer / Runtime Environment (RTE)

- Finalize concept and design for integration & test.
- Dependency analysis, adaption needs (based on TAS Platform details as provided in the trainings), integration, commissioning, and test with simulation.

Q1/2024 / M15 to Q1/2025 / M27: MDCM Services Development, Provision, Integration, Commissioning, Adaption & Test

- Finalization of MDCM subsystem design & functional description.
- Concept and design for integration & test.
- Adaption towards Safety Layer / Runtime Environment (RTE) for integration and adaption of existing TAS Platform diagnostics services for syslog access, usage of SNMP or other TAS Platform interfaces
- Execution of integration & test.

Q1/2025 / M27 to Q2/2025 / M30: DIA over FRMCS

- OBapp implementation (service stratum), based on (reference) OBapp agent implementation.
- Realization of communication over FRMCS (transport stratum) to wayside.
- Realization of communication path TCMS Data Service → DIA-VEC → lab frontend / dashboard (visualization of vehicle data) as trackside entity.

Q2/2025 / M31: Integration of final TCMS Data Service Version (deliverable 31.3)

- Transfer the final TCMS Data Service implementation to work package 36 demonstrator setup.

from Q3/2025 / M33 onwards: DIA Services towards Applications

- Realization of application diagnostics user stories on Demo Applications in cooperation with the SBB.
- Demonstration of possible software update workflow (for configurations, applications, and operating systems) and gap analysis to onboard standards that might be in process or specified in the meantime.

→ Results:

- M27: Definition of diagnostics interface towards demo applications available and tested.
- M31: DIA service interface implementation integrated.

3.4 Test Environment

The test environment adds the sub-systems to the demonstrator setup that are needed to establish the relevant environment for the modular computing platform. In this sense those sub-systems are at or on the boundary of the system under consideration and are implemented up to TRL 5.

Some of the sub-systems include parts outside the system under consideration which are implemented in the demonstrator setup as simple mockups or simulations with the sole purpose of providing test data / responses to the system under consideration or to visualize test results.

3.4.1 Onboard Communication Network

→ Overall responsibility: SMO

→ Objectives:

- Demonstrate the integration of a modular computing platform with an UNISIG SUBSET-147 compliant CCS Consist Network (CCN).
- Enable the communication of applications on the modular computing platform with other entities in the onboard domain or via FRMCS TOBA & Trackside Entity to trackside.

→ Preconditions:

- Specification of UNISIG SUBSET-147 OSI layers 1-2 is available with TSI 2023.
- Proposal on specification of UNISIG SUBSET-147 on OSI layers 3-6 (1-6 in total) is available in M20.
- UNISIG SUBSET-147 CCN example configuration is available from work package 23. (As far as feasible, this demonstrator implements the specifications of UNISIG SUBSET-147 that are expected to further be detailed in future versions during the runtime of the work package.) This includes an example configuration of the following demonstrator setup in a physical lab environment:
    - Core network
        - 6 Advanced Physical Layer (APL) ethernet switches, TSI 2023 compliant
        - Switches are industry-grade, but for lab flexibility reasons have RJ-45 connectors instead of M12 (deviation from TSI 2023). (Identical switches with M12 and rail-grade environment specification are available, so no impact on applicability of results.)
        - Core topology: ring type. Redundancy mechanisms in place.
    - Multiple VLANs statically configured in the core network

- Quality of Service (QoS) classes statically assigned to VLANs (each VLAN gets assigned one QoS class)
- Demonstrator level implementation of shared services for
  - Dynamic Host Configuration Protocol (DHCP)
  - Domain Name Server (DNS)
  - Network Time Protocol (NTP)
  - Radius based authentication backend

→ Work items:

Q3/2024 / M21-M23:

- Transfer demonstrator configuration of work package 23 to work package 36.
- Setup and configuration of the UNISIG SUBSET-147 compliant CCN in the Physical Lab Environment.

Q3/2024 / M21 onward:

- Consulting for implementation of a UNISIG SUBSET-147 compliant communication gate as Model 3 task set on the TAS Platform.
- Consulting for adaption of the Train Adapter / TCMS Data Service to adhere to UNISIG SUBSET-147.
- Consulting in the possible addition of a security gateway to the network to separate security zones.

→ Results:

- M24: Running CCN demonstrator in Physical Lab Environment

3.4.2 FRMCS TOBA & Trackside Entity

→ Overall responsibility: Kontron

→ Objectives:

- Provision of an FRMCS onboard setup, capable of simulating an end2end FRMCS communication.
- Including a wireless communication (WIFI) as transport layer bearer for FRMCS communication for test / presentation purposes.

→ Preconditions:

- Physical Lab Environment providing
  - Space for TOBA box installation
  - Connection to Kontron labs (A and F)
  - Trackside WIFI access point
  - Server for trackside gateway including an environment for the deployment of virtual machines

→ Work items:

Q3/2024 / M21:

- Provision and installation of TOBA box.
- Lab setup in Kontron A for MCx server.

- Setup of the remote connection (VPN) from the Kontron lab to the Physical Lab Environment including the trackside gateway.

Q1/2025 / M28:

- Study to which extent and how onboard FRMCS TOBA functions could be split, with parts of the functions possibly hosted on the same hardware pool as the Modular Computing Platform and decupling of the modem hardware (e.g., with OBrad if available) via the CCN.
- Study on possible redundancy of TOBA / modem hardware and fallback logic on Modular Computing Platform to increase availability of the FRMCS connection.

→ Results:

- M26: TOBA hardware with WIFI modem and “trackside” WIFI module supplying the MCx server (via VPN to Kontron lab).
- M28: Integration according to UNISIG SUBSET-147 on OSI layers 1-3.
- M35: Study results on possibility to host (parts of) the TOBA software on the Modular Computing Platform and decupling of the modem hardware (e.g., with OBrad if available) via the CCN.
- M35: Study results on possible redundancy of TOBA / modem hardware.

3.4.3 Train Adapter / TCMS Data Service

→ Overall responsibility: DB

→ Objectives:

- Simulate the connection to the train TCMS by standardised basic integrity train abstraction interfaces.

! So far, no partner in the work package can provide a safe Functional Vehicle Adapter (FVA).

→ Preconditions:

- Standardised specifications for a (basic integrity) train abstraction interface (e.g., EuroSpec TCMS Data Service) is available.

→ Work items:

Q1/2024 / M16:

- Deployment of a TCMS simulation and TCMS Data Service in the Virtual Lab Environment.

Q2/2025 / M31:

- Deployment of the final TCMS Data Service version from work package 31 in the Physical Lab Environment.

→ Results:

- M16: Preexisting TCMS Data Service is available in the Test Environment on the CCN.
- M31: TCMS Data Service is updated to final version from work package 31.

! Vehicle abstraction for safety critical functions cannot be demonstrated due to a missing partner that could provide the needed Functional Vehicle Adapter (FVA) software.

3.4.4 IT/OT Security

→ Overall responsibility: Shared

→ Objectives:

- Consolidate existing IT/OT security considerations applicable to the Modular Computing Platform.
- Identify and define needed sub-systems to ensure IT/OT security of the Modular Computing Platform.
- If applicable: Demonstrate the integration of such sub-systems in the demonstrator setup.

→ Preconditions:

- Onboard Communication Network is specified and a readily configured setup is available in the Physical Lab Environment until M30.
- Security assessments and certifications of the TAS Platform are provided by GTS.
- Application (data) security requirements are specified (e.g., derived from safety requirements).

→ Work items:

Q1/2024 / M14:

- GTS: Provide existing security handbooks and certifications of the TAS Platform components deployed in the demonstrated setup.
- DB/SBB: Risk assessment and assessment on protection needs based on proposed system architecture and demo applications.

Q1/2025 / M26:

- SBB/SMO: Decision on the possible integration of a "security gateway" / firewall to separate different zones of the Onboard Communication Network.

→ Results:

- M16: Document collection on existing security considerations of the sub-systems in the demonstrator setup.
- M25: Security risk assessment on the demonstrated system architecture.
- M30: Final conclusion on security consideration for the Modular Computing Platform and possibly the demonstrated integration of a separation of network zones in the Onboard Communication Network.

3.5 Demo Applications

In contrast to the previous areas in this implementation plan, the demo applications have no outgoing dependencies towards systems that rely on their (timely) implementation. The demo applications are rather means to provide realistic show cases in which the user stories of the demonstrator can be tested and presented.

The demo applications are implemented as simple application dummies with minimal functional scope. They are not meant to provide any functional value but follow the purpose to serve relevant workloads to the Modular Computing Platform as well as utilize platform and communication services. In this sense, also parts of Monitoring, Diagnostics, Configuration and Maintenance

(MDCM) – like the DIA-VEC – can be considered as demo applications since they also run on the Modular Computing Platform.

No certification or homologation is planned for any of the demo applications, nor does their development strictly follow EN 50126, EN 50128, EN 50129 and EN 50159 safety standards or IEC 62443 security standards.

3.5.1 ATO Control Loop

→ Overall responsibility: SBB

→ Objectives:

- Present a running basic integrity application for a non-safety relevant function on the Modular Computing Platform communicating via FRMCS with a trackside entity and via the TCMS Data Service to a TCMS simulation.

→ Preconditions:

- TAS Platform development training by M14.
- Configuration Management tools and processes available by M30.
- Virtual Lab Environment with Safety Layer / Runtime Environment (RTE) for early testing available by M21.
- Physical Lab Environment with Safety Layer / Runtime Environment (RTE) for integration testing available by M30.
- FRMCS Platform Functions including OBapp gate is available and tested by M30.
- FRMCS TOBA & Trackside Entity and TCMS Data Service integrated as test environment by M31.

→ Work items (all done together with ETCS Control Loop):

Q1/2024 / M14 to Q3/2024 / M20: Prepare collaboration

- Decide about model of collaboration for work package task 36.4.
- Start procurement of application development.

Q3/2024 / M21 to Q2/2025 / M30: Prepare development

- Create functional specification of ATO Control Loop and other involved components (e.g., TCMS simulator, ATO trackside simulator).

Q2/2025 / M30 to Q1/2026 / M40: Realization / development

- Realize the ATO Control Loop application and the other involved components identified before.
- Execute intensive testing of ATO Control Loop in the fully integrated demonstrator setup.
- Demonstrate the ATO Control Loop functionality to an audience.
- Identify weaknesses and possible improvements, mainly in respect to the used platform solution.

→ Results:

- M36: Insights and learnings for further improving the modular computing platform concepts.
- M40: Raised awareness and marketing for the approach of an onboard modular computing platform.

3.5.2 ETCS Control Loop

→ Overall responsibility: SBB

→ Objectives:

- Present a running safe application for a safety relevant function (i.e., SIL 4) on the Modular Computing Platform communicating via FRMCS with a trackside entity and via a safe I/O to a TCMS simulation.

→ Preconditions:

- TAS Platform development training by M14.
- Configuration Management tools and processes available by M30.
- Virtual Lab Environment with Safety Layer / Runtime Environment (RTE) for early testing available by M21.
- Physical Lab Environment with Safety Layer / Runtime Environment (RTE) and safe I/O for integration testing available by M30.
- FRMCS Platform Functions including OBapp gate is available and tested by M30.
- FRMCS TOBA & Trackside Entity integrated as test environment by M31.

→ Work items (all done together with ATO Control Loop):

Q1/2024 / M14 to Q3/2024 / M20: Prepare collaboration

- Decide about model of collaboration for work package task 36.4.
- Start procurement of application development.

Q3/2024 / M21 to Q2/2025 / M30: Prepare development

- Create functional specification of ETCS Control Loop and other involved components (e.g., TCMS I/O simulator, ETCS trackside simulator).

Q2/2025 / M30 to Q1/2026 / M40: Realization / development

- Realize the ETCS Control Loop application and the other involved components identified before.
- Execute intensive testing of ETCS Control Loop in the fully integrated demonstrator setup.
- Demonstrate the ETCS Control Loop functionality to an audience.
- Identify weaknesses and possible improvements, mainly in respect to the used platform solution.

→ Results:

- M36: Insights and learnings for further improving the modular computing platform concepts.
- M40: Raised awareness and marketing for the approach of an onboard modular computing platform.

3.5.3 Digital Register

→ Overall responsibility: DB

→ Objectives:

- Present the communication of a safety relevant application on the Modular Computing Platform with a trackside entity via FRMCS.

- Visualize the safety response of the Modular Computing Platform to hardware and software failures.
- Demonstrate safe data persistence.

→ Preconditions:

- TAS Platform development training by M14.
- Deployment of Safety Layer / Runtime Environment (RTE) on Virtual Lab Environment and Physical Lab Environment by M30.
- FRMCS Platform Functions including OBapp gate is available and tested by M30.
- FRMCS TOBA & Trackside Entity integrated as test environment by M31.

→ Work items:

Q1/2024 / M15:

- Assess feasibility to port (parts of) the dbs-onboard-map-api to a Model 1 task set on the TAS Platform.

Q2/2024 / M17 to Q2/2025 / M29:

- Raise the necessary budget and potentially procure external resources to execute the needed development.

Q2/2025 / M30 to Q1/2026 / M40:

- If feasible within the work package resources
    - Implement a safe onboard map cache as Model 1 task set on the TAS Platform.
    - Deploy the dbs-onboard-map-api mock server on the trackside entity.
    - Execute integration tests in complete demonstrator setup, possibly enhanced by additional test equipment to visualize the map data.
    - Develop a setup for presentation purposes.

→ Results:

- M40: (given economic feasibility) Minimal implementation of a safe onboard map cache according to the dbs-onboard-map-api that can be used to showcase the Modular Computing Platform and (possibly redundant) FRMCS communication to a trackside server.

4 VERIFICATION AND VALIDATION

For each chapter in the Implementation Plans the partner holding the overall responsibility is accountable to facilitate reproducible integration tests that prove the completion of the named results. Within the time span of an implementation task (36.2 to 36.4) the task leaders are responsible to coordinate such tests and handover their status to the proceeding task leader.

To verify and validate the general demonstrator user stories, some individual test cases are already defined respectively in the User Stories & Test Cases document. Each of those test case is assigned to one of the partners who is responsible for its execution. A summary of the conducted tests and their results are included by the coordinating task leader in a report as part of the deliverable of the respective task.

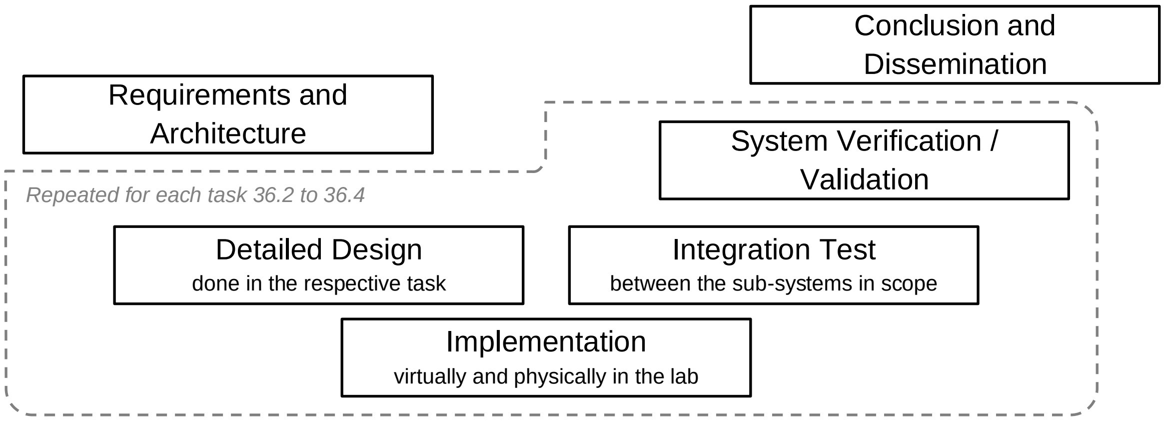

Figure 2: Diagram of the Process Model

The system architecture for the demonstrator is defined in task 36.1 and subsequently validated against the user stories with each implementation task up to the extent of the demonstrator setup completed in the respective implementation task. While new sub-systems are integrated along the way their integration is individually tested – independently of the user stories and their test cases – to ensure their proper behaviour in further tests.

All test procedures are documented together with the respective test data and test results in the appropriate Configuration Management tool. If possible, unit and integration tests are automatised and included in the CI pipelines for the respective sub-system.

5 COLLABORATION

While for practical reasons the Implementation Plan defines a clear work split between the partners in accordance with their respective expertise, all partners commit to support each other in the completion of the work items stated above. Preconditions and dependencies are stated in good faith to clarify interfaces and work handovers and do not externalize risks. It is the duty of all partners to address identified risks and to contribute to their mitigation.