Rail to Digital automated up to autonomous train operation

D31.1 – ATO Onboard and Remote Supervision & Control strict formal model demonstrator process description

Due date of deliverable: 30/05/2026

Actual submission date: 30/05/2026

Leader/Responsible of this Deliverable: Dr. Simon Funke (DB Cargo AG)

Reviewed: Y

Document status		
Revision	Date	Description
01	31/07/2025	First WP internal draft
02	27/03/26	Internal draft for WP review
03	30/04/26	Version available for TMT review
04	22/05/26	Version after SteCo review
05	14/07/26	Version after external review (minor corrections)

Project funded from the European Union's Horizon Europe research and innovation programme		
Dissemination Level		
PU	Public	PU
~~**SEN**~~	Sensitiv – limited under the conditions of the Grant Agreement	

Start date: 01/12/2022 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
Dr. Simon Funke	DB Cargo	Lead author
Thomas Jousselin	SNCF	Review
Patrick Rozijn	NS	Review
Miguel Fernández	Cedex	Review
Pablo Domínguez	Ineco	Review
Robert Grosser	SMO	Review
Xiaolu Rao	SBB	Review
Giuseppe Guida	HITACHI STS	Review

EXECUTIVE SUMMARY

The application of formal methods within the railway sector has emerged as a pivotal strategy to enhance the safety, reliability, and efficiency of railway operations. Over the past few years, significant advancements in automatic functions have been made, such as the development of Automatic Train Operation (ATO) systems which promise increased operational consistency and reduced human error. However, more understanding is necessary of the necessary interfaces of different subsystems that were mainly vendor specific in the past. This remains a challenge especially for the application of ATO in the freight. E.g. the freight demonstrator in S2R running between Sion and Sierre in Switzerland [1] revealed some gaps in the specifications, e.g. in UNISIG Subset 125, that were resolved only partially until today (current version is 1.1.0). Current specifications, e.g. for ETCS and ATO are described in textual form and thus not fully formalized. This leaves room for interpretation.

As the industry moves towards these automated solutions, specifying interfaces for ATO systems is becoming increasingly critical. This document offers a comprehensive process description, detailing the tools employed and lessons learnt in formal modeling with a focus on ATO Onboard and Remote Supervision & Control / Remote Train Operation (RTO) in freight operations. Building upon the OCORA experience as well as further work, as e.g. described in FP2 D5.5, this document delivers a formal ATO model process description for testing and reference purposes. It targets two subtopics to encompass a broad spectrum of ATO deployment types. These include the development for GoA4 and remote operation on mainline operation and GoA2 in passenger missions utilizing diverse development environments such as SCADE and Simulink.

The current document focuses on the mainline operation use cases, while the other use case – along with an additional analysis of GoA4 on technical movement for passenger trains – is analyzed in D31.5. The two documents highlight the versatility in formal modeling suited to varied domain requirements. The work is implemented in SCADE since it covers the full lifecycle of the V-model, conform to EN 50716. The added value of this document lies within providing a model description for the formal modeling of freight specific use cases, thus fostering enhanced collaboration in the railway industry. Finally, since a common definition of remote train operation (RTO) was not available, but needed for this work, a definition proposal is made.

ABBREVIATIONS AND ACRONYMS

AD	Automatic Driving
ADM	Automatic Driving Module
APM	Automatic Processing Module
ALM	Application Lifecycle Management
ASR	Additional Speed Restriction
ATO	Automatic Train Operation
ATO-OB	Automatic Train Operation – On Board
ATO-TS	Automatic Train Operation – Track Side
ATP	Automatic Train Protection
ATP-OB	Automatic Train Protection – On Board
ATSM	Automatic Train Stopping Management
AUGT	Automated Urban Guided Transport
CCS	Control Command and Signalling
CCTV	Close-Circuit TeleVision
CCU	Central Control Unit
CENELEC	European Committee for Electrotechnical Standardization
DMI	Driver Machine Interface
DSE	Driving Style Engine (Extended Profile Calculation for Freight Operation)
EB	Emergency Brake
ECM	Entity in Charge of Maintenance
EMU	Electrical Multiple Unit
EOA	End Of Authority
EOJ	End Of Journey
ERA	European Railway Agency
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETCS-DMI	European Train Control System – Driver Machine Interface
ETCS-OB	European Train Control System – On Board system
FFFIS	From Fit Functional Interface Specification
FIS	Functional Interface Specification

FP2	Flagship Project 2 (FP2-R2DATO)
FRMCS	Future Railway Mobile Communication System
FS	Full Supervision
GoA	Grade of Automation (1 to 4)
GUI	Graphical User Interface
HMI	Human Machine Interface
IEC	International Electrotechnical Commission
IM	Infrastructure Manager
ISM	Incident Solving Manager
ISO	International Organization for Standardization
JP	Journey Profile
JU	Joint Undertaking
L2	ETCS Level 2
LS	Limited Supervision
MBSE	Model Based System Engineering
MD	Mission Data
MDS	Multi Display System
MNC	Mastership Negotiation Component
MP	Mission Profile
NTC	National Train Control
NVR	National Vehicle Register
OA	Operational Analysis
OAS	Onboard Automation System
OB	On-Board
OCORA	Open CCS Onboard Reference Architecture
ODR	Onboard Driver
ORD	Onboard Recording Device
ORDM	Onboard Remote Driving Manager
OS	On-Sight
PER	PERception
R2DATO	Rail to Digital automated up to autonomous train operation
RC	Remote Control
RD	Remote Driver

REP	REPository
RINF	Register of INFrastructure
RSC	Remote Supervision Center (acc. to GA, formerly used for RTO)
RST	Rolling stock -[SS-139]'s abbreviation for TCMS
RTO	Remote Train Operation
	Implementation Context: RTO-L2-FS-AD ETCS Level 2, AD Mode as backup for ATO-GoA-4 Operation
RTO-OB	Remote Train Operation – Onboard
RTO-TS	Remote Train Operation – Track-Side
RU	Railway Undertaking
SIL	Safety Integrity Level
SP	Segment Profile
SR	Staff Responsible
SRS	System Requirements Specification
TBL	Traction/Braking Lever
TCMS	Train Control Monitoring System
TMS	Traffic Management System
TRL	Technology Readiness Level
TS	Trackside
TSI	Technical Specifications for Interoperability
TSI OPE	TSI Operation and Traffic Management
TSI TAF	TSI Telematics Applications for Freight
TSI TAP	TSI Telematics Applications for Passengers
UIC	Union Internationale des Chemins de fer
X2RAIL	Shift2rail project identified by the grant agreement n881806

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The present document constitutes the Deliverable D31.1 “ATO Onboard and Remote Supervision & Control strict formal model demonstrator process description” in the framework of the Flagship Project FP2- R2DATO as described in the EU-RAIL MAWP (Multi-Annual Work Programme). The document describes results for the Task 31.1 “ATO Onboard & Remote Supervision & Control”. WP31 is part of the FP2 cluster (4) “Fast and effective deployment” containing the four technical enablers (TE): TE15 DevOps/Architecture4Evolution, TE19 Modeling techniques, TE20 Deployment and migration, and TE14 testing, validation and certification.

The objective of this document is to provide a process description of the application of formal methods to the development of automating functions in the railway sector. To represent different parts of the sector, WP31 defines two different use cases: one in the freight and one in the passenger sector. This deliverable focuses on the freight use cases. The process description of the passenger use case can be found in D31.5 “Use case YTSM model report". Rail (freight) systems comprise a wide range of automation process tasks, reaching from communication and perception systems to remote supervision and control as outlined in the document.

The following results rely on a broad body of existing knowledge, especially from previous European research activities (e.g., from S2R, OCORA) as well as the expert knowledge from the involved partners. The main input comes from operators, defining the use cases, the resulting operational scenarios as well as the modeling itself. The underlying use case, “ATO Onboard and Remote Supervision”, was developed by DB Cargo and is based on previous work, specifically done in OCORA and based on requirements and resulting design decisions as presented in the FP2 deliverable D5.5. In contrast to other deliverables of WP5, that developed use cases that were further developed into requirements and specifications in WP6, D5.5 defined already (freight specific) user requirements that did not need to be further detailed out in WP6. This document describes the process of MBSE for freight ATO and RTO for mainline applications. The results are purely illustrative; they have not been verified and are not final. This work is not aligned with the “ATO-Cargo” project consortium which will continue until 06/27.

The main goal of the presented work as well as its added value compared to previous work is given in chapter 4 along with the methodology to obtain a process description of the application of formal methods in the rail freight sector, allowing for deducing lessons learnt for the development process as well as for the identification in insufficiently defined specifications that need to be adapted for a functioning collaboration of different subsystems. In addition, the challenges of driving freight trains automatically (ATO and RTO) are presented as background. Further, a proposal for a definition of remote driving is given. The emphasis of this work is to give a methodological framework for model based systems engineering in the rail sector. In a more FP2-R2DATO context, the work is compared to deliverables from WP6.

2 OBJECTIVE / AIM

The main goals of this work are:

- Definition of two basic use cases that were modeled. Use cases build the basis for the modeled functions and systems. Key outputs are the process description, including exemplary sequence diagrams
- Description and reasoning of the tool chain used
- The output of this work is the process description and not the formal model itself. Key outputs are thus the process description itself as well as the lessons learnt of their application, especially in the light of two different approaches. It provides a comprehensive guide and demonstration of the formal modeling process, adding value by enhancing the reliability and testability of ATO systems.
- The developed process description shall be used to build models to verify and validate the design and specifications, also for freight

2.1 TASK DESCRIPTION

Task 31.1 started in month one and the outputs of this task are included in this document. The following table gives the direct match of the task definition from the Grant Agreement with the output and a link to the section where more details can be found. Grayed-out passages refer to the general WP description that can be seen as a more general reference to the methodology. However, also these aspects are covered by this document as referenced in the right column of the following table. The mentioned TCMS formalisation is exclusively part of task 31.2 and thus, not part of this deliverable.

	Definition from Grant Agreement	Reference in D31.1
WP31	This WP builds upon the objectives and principles of WP 30 and extends it further. In particular, this work package is focused on delivering and developing (a) a functional correct model process description for ATO Onboard and Remote Supervision & Control, and (b) formal modeling and specification of TCMS Data Service. Expected output includes process description of digital CCS+ models, created to: • Establish better design and engineering requirements process • Benefit from activities such as prototyping (by means of animation / specifications), definition of test cases, refinement, support of safety argumentation, etc. • Form an integral part of safety argumentation, e.g., evidence that safety requirements derived from risk assessment and hazards hold	2.2.1 Formal methods in FP2 2.2.2 Way of working: Applying formal methods in FP2 T31.1 7 Conclusion and recommendations

	Definition from Grant Agreement	Reference in D31.1
	The WP Modeling techniques will aim to provide a clear and unambiguous interface to stakeholders including suppliers. To ensure different organisations can leverage the benefits, modeling techniques must align with modern software development practices, such as agile methods and the key principles of DevOps: shared ownership, workflow automation, and rapid feedback. The following goals should be achieved along the V cycle: • Apply modeling throughout the V-cycle, including use of MBD tools • Support transformation of semi-formal models to executable/testable/formally verifiable models by process description • Give an outlook on verification and testing • Consider accounting for requirements of safety, cybersecurity & human factors	4 Methodology 4.1 Advanced Modeling Techniques
T31.1	This task will build upon OCORA experience and tooling and will evolve in alignment with System Pillar's Architecture standards and tooling to produce a strict formal ATO Onboard and Remote Supervision & Control model process description for testing and reference purposes. Two subtopics will be implemented: A subtopic on freight train RSC, led by DB. A subtopic on GoA4 for technical movements and GoA2 for passenger missions, led by SNCF. These two subtopics will enable coverage of a wide spectrum of ATO deployment types. They will also demonstrate the modeling approach using different development environments, reflecting the diversity found in the industrial domain (SCADE and Simulink).	2.2.2 Way of working: Applying formal methods in FP2 T31.1 2.3 State of the Art 2.3.2 OCORA 5 Scope of modeling 4 Methodology & D31.5
D31.1	Based on existing tools and standards, a process description for a fully formal chosen model demonstrator	This whole deliverable represents the corresponding process description

Table 1: Deliverable sections matching task description

2.2.1 Formal methods in FP2

Gaining more product maturity, automatic driving functions shall apply formal methods for their development. In FP2-R2DATO, various aspects of the model-based system engineering approach (MBSE) are included, such as the definition of use cases and user requirements in WP5, the definition of specifications for the different subsystems as well as architecture development in WP6. However, the developed technologies and prototypes in FP2 are developed concurrently and thus do not follow the corresponding specification. Similarly, this work package started in month one and was developed in parallel. For the application of formal methods, in FP2-R2DATO especially the two work packages 30 and 31 were designed. These showcase the potential for specific use cases. The following figures show the discussed relations.

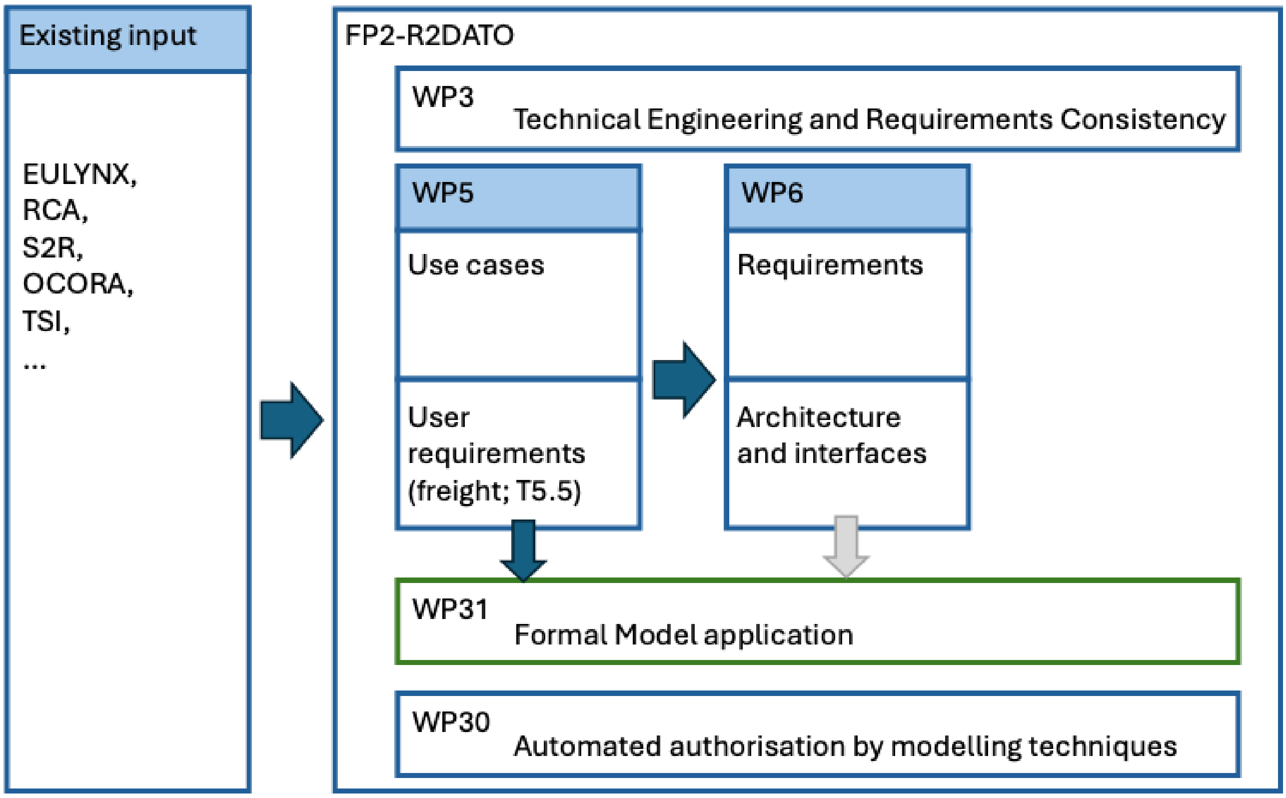

Figure 1: FP2 T31.1 Project relations

2.2.2 Way of working: Applying formal methods in FP2 T31.1

In Task 31.1 formal methods will be applied to two different use cases:

1. ATO mainline and remote supervision (see also D5.5 [3] for details)
2. Yard to station movement (see also D31.4 and D31.5)

For the application of the formal methods to the use cases, DB Cargo and SNCF are responsible for Use Case 1 and Use Case 2, respectively. Results were developed by these two entities and discussed within the task with the different partners, reflecting their different backgrounds and their specific ideas and goals.

The development of this task is based on work done before, especially in the context of (past) European funded projects (see also chapter 2.2.1 and 2.3). To capture and align with the different perspectives of all task participants, bi-monthly meetings are held. Regarding this deliverable, especially the early provision of a task internal version 0.1 supported the alignment. Finally, the alignment with other work packages and other stakeholders such as the System Pillar is necessary to ensure alignment beyond the Work Package.

The three process steps are summarized in Figure 2.

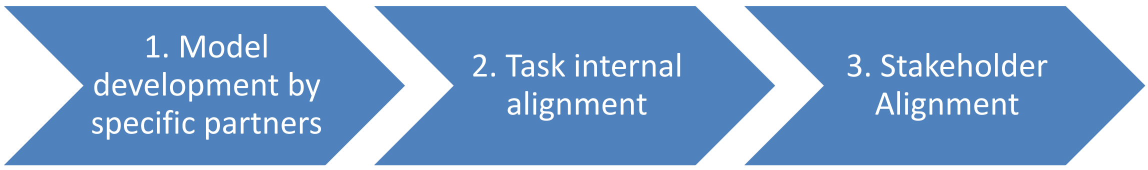

Figure 2: FP2 T31.1 Process steps

1. Model development
   As an input to the task, use cases and user requirements from previous research activities in the European context (e.g., from S2R, FP2 D5.5) as well as the expert knowledge from within the involved operators were gathered.
2. Task internal alignment
   The user requirements described in this document cover grades of automation GoA2 to GoA4 and remote supervision targeting of full automation of the freight sector. Bi-monthly meetings and the early provision of an internal working document facilitates the task internal alignment.
3. Stakeholder Alignment
   Within this context, the alignment with the FP2 WP6 (“Automation Processes Specifications”) was especially important.

2.3 State of the Art

The reasoning behind the work of this document is already well described by OCORA [6]:

“Current ETCS documentation (Subset 026, 034, 119, etc.) is expressing the system requirements in textual form. Although these specifications are quite comprehensive, they still leave room for interpretation (problem #1) and are lacking details in some cases (problem #2). In addition, the sheer number of specifications naturally causes inconsistencies (problem #3) and creates risks for errors during implementation (problem #4). As a result, testing and certification efforts increase accordingly (problem #5). All this may lead to quality and performance issues and generates very high total costs of ownership for ETCS on-board solutions.

To overcome the issues mentioned, it is important to decompose the CCS on-board system in well specified components / building blocks (refer to System Architecture documentation [13] for details) and to use MBSE to develop the needed specifications for all building blocks. The resulting model is intended to amend the current TSI specifications with the necessary details allowing CCS system or component providers to implement high quality ETCS on-board systems at a competitive price. Furthermore, MBSE based simulations will help reducing the test and certification effort."

For the state of the art of automatic verification, please refer to FP2-R2DATO D30.2. For the work done in WP6 and the relation to work done in previous projects of X2Rail, please refer to chapter 6.5, as well as WP6 deliverables (e.g. references [11, 12]).

2.3.1 ATO Systems

For a general description of the status quo of ATO systems in general, please refer to D5.5 [3] which constitutes the reference of this deliverable. For better reference, the overview of the ATO functionalities is quoted in the following, for further details refer to [3]. Please note, the following paragraph is given as a general reference and does not constitute a technical contribution.

The components of a potential ATO solution for rail freight consists of the following functionalities:

1. European Train Control System (ETCS)
   Train protection system.
2. ATO onboard System (ATO-OB)
   Locomotive component, e.g., for automated driving and braking.
3. ATO trackside (ATO-TS)
   Interface between the ATO-OB and the IM
4. Perception system
   Specified perception functions
5. Remote Train Operation (RTO) (formerly Remote Supervision & Control (RSC))
   remote control for all ATO level and control e.g. in case of "degraded mode" for GoA 4.
6. Driving Style Engine (DSE): Functionality to control and supervise freight specific driving style requirements.
7. Functional Vehicle Adapter FVA: Specific adapter as translator from generic ATO OB to Vehicle specific Locomotive system.

Driving operation will ideally be relying on ATO. However, while this will apply on nominal operation, there must be a fallback-option in degraded mode. Remote Train Operation, RTO, or Remote Supervision and Control (RSC) is meant as such a fallback option where a remote driver can remotely control the train to manage the situation. In this position, a person remains the highest decision-making authority of the railway system.

The RTO center will be a new work environment with new roles. Accordingly, the driver´s job description needs to be adapted as well as the organizational structure within the railway undertaking.

A basic specification of a remote driving system is currently developed within the scope of European research (Shift2Rail, IP2 X2Rail4 and IPX TAURO). The system has achieved at least TRL 4. In addition, Thales / Vodafone 5G driverless driving in the Ore Mountains as well as SNCF Train Autonome in France have tested remote driving.

Remote driving shall resolve malfunctions for GoA4 with an unoccupied locomotive. As such, it is an essential function of the ATO system.

2.3.2 OCORA

OCORA is an important input to this work – see Figure 1. In the following, OCORA is shortly described based on publicly available OCORA documents.

Europe is investing in the development of a Single European Rail Area (SERA) to achieve its political objectives. These investments focus on research, development, and innovation to maintain the railway community's competitive edge through initiatives like Shift2Rail and its successor, as well as supporting technological progress. This involves implementing ERTMS/ETCS and transformative technologies like ATO and FRMCS. However, SERA has not yet been fully realized due to ongoing barriers such as national technical and operational rules along with legacy CCS systems, which hinder a unified railway system. Europe's primary goals are to eliminate country or network-specific solutions in these areas. OCORA aims to provide an architectural framework for on-board systems to support this European integration, beginning with managing existing legacy infrastructures, such as ERTMS and train-borne ETCS installations. [4, p. 6]

To address challenges in the European railway sector, a coherent, modular, upgradeable, interchangeable, reliable, and secure system architecture is crucial. The intent is to establish the Open CCS On-board Reference Architecture (OCORA) to complement the trackside control-command and signalling subsystem. OCORA is designed to effectively mitigate risks but does not claim to solve all issues independently. It relies on close cooperation with stakeholders to collaboratively advance automation and digitalisation in European railways. [4, p. 7]

Besides its agile process with on-demand release cycles, OCORA follows a longer-term planning road map as presented below. The timeline of EU-Rail initiatives is also shown for direct comparison.

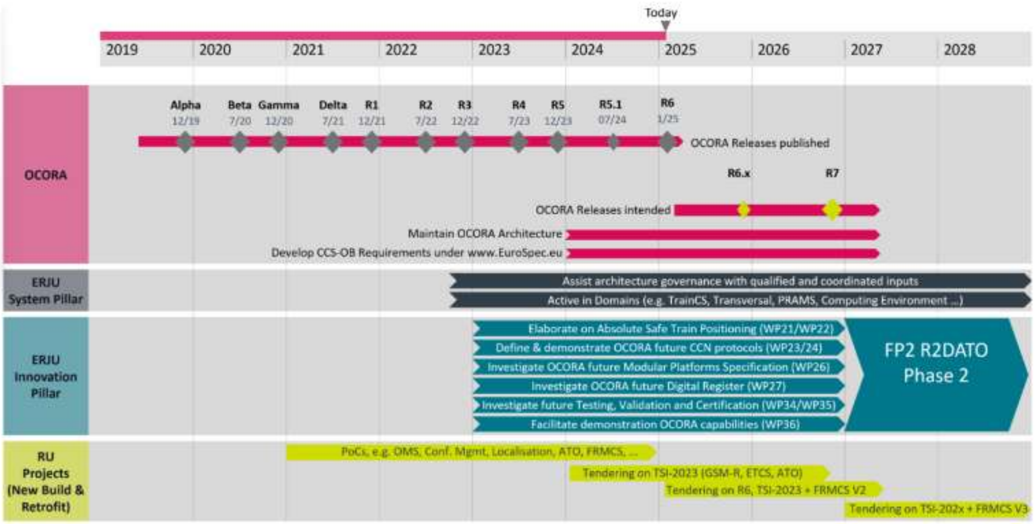

Figure 3: OCORA Road Map [5]

3 REGULATIONS, OBSTACLES AND CHALLENGES FOR FREIGHT ATO GOA4

The existing European architecture harmonises ATO only up to GoA2, with Subset-125/126 and related TSI OPE procedures assuming a human operator remains involved. Certain ETCS-L2 corridors—such as those published via RINF—already expose prerequisites for ATO deployment (e.g., support for ATO functions or train-integrity requirements), yet national rules continue to govern critical elements like emergency communication. As a result, unattended freight remains outside full European harmonisation.

Especially with regard to the GAP analysis to the outputs of WP 6.5 and WP 6.8 (see chapter 6), this MBSE analysis identifies where adaptations are required to support GoA4/RTO scenarios. Key changes for automated freight operation relate to:

• Improved train dynamics model considering the different brake systems of freight trains

• the mandatory availability of detailed freight-train data (e.g., consist, weight, wagon characteristics),

• operational and driving-rule constraints,

• ATO engagement prerequisites,

• defined procedures for boarding and deboarding,

• external locomotive status indication,

• external override for boarding/deboarding, and

• pre-movement warning functions.

3.1 DRIVING RULES AND OPERATIONAL LIMITATIONS OF FREIGHT TRAINS

Freight trains show specific behavior that needs to be addressed for automatic driving of freight trains:

- Long freight trains transmit forces through many couplers and are highly dynamic. Accordingly, traction and brake application need to be adapted for this specific behavior.
- Freight Trains use different brake systems under different conditions. The use of the electrodynamic brake is energy efficient and therefore may be preferably used where possible and admissible.
- Holding and starting heavy freight trains in slopes needs specific consideration.
- Freight locomotives need safety measures to warn staff nearby before automatic movement start of the locomotive.
- Freight locomotives need safety measures to allow for a safe boarding and deboarding of personnel.

These challenges need to be addressed and can be modeled. However, specific solutions still need to be verified. Further developments are ongoing.

3.2 Regulatory open points and challenges

For ATO GoA4 and RTO operation of freight trains, mainly the following challenges arise:

1. Human centered rules: OPE’s harmonised rules demand driver presence; unattended operations lack harmonised replacements for European Instructions, degraded-mode handling, and SR/EOA processes.
2. Standards ceiling at GoA2: The UNISIG ATO baseline (Subset 125/126) explicitly stops at GoA2; GoA4 needs new specifications and/or ERA guidance for remote role, safety responsibilities, and handovers.

Affected regulations comprise, but are not limited to, TSI OPE, TSI CCS, UNISIG Subset 026, 125, 126, 139. Further analyses are ongoing.

4 METHODOLOGY

Model-based systems engineering (MBSE) is an interdisciplinary approach for developing complex systems using visual modeling techniques to describe them from different perspectives. The aim is to create a consistent system model that offers specific views for various purposes. This ensures traceability of requirements, design elements, analysis, and tests, with development artefacts generated directly from the model as the single source of truth. MBSE relies on three pillars: Tool, Language, and Method, which include Framework and Process components. The Tool is software for creating the virtual model. The Method defines how to use the Tool and Language to achieve the desired goal. The Framework provides the basic structure and meta-model, while the Process details the steps, roles, actors, and artifacts involved in system modeling.

4.1 ADVANCED MODELING TECHNIQUES AND TOOLING

In this section, we describe the approach used in the modeling toolchain for the ATO Onboard and Remote Supervision & Control systems. The aim is to ensure reliable and verified systems using formal modeling techniques coupled with stringent requirements management.

The design process guideline highlights the use of sequence diagrams and activity diagrams to represent system behaviors. Each use case is thoroughly detailed using these diagrams, which define the start and end conditions and involve various external actors and entities. The process meticulously refines high-level requirements into operational scenarios that are translated into system functionalities. These functionalities are depicted through internal block diagrams, illustrating interfaces and flows. The logical architecture is derived from these requirements to bridge system functionalities with software or hardware implementations, while considering modularity and interface complexity. This method ensures consistency and provides an extensive view of the system's operational and functional aspects.

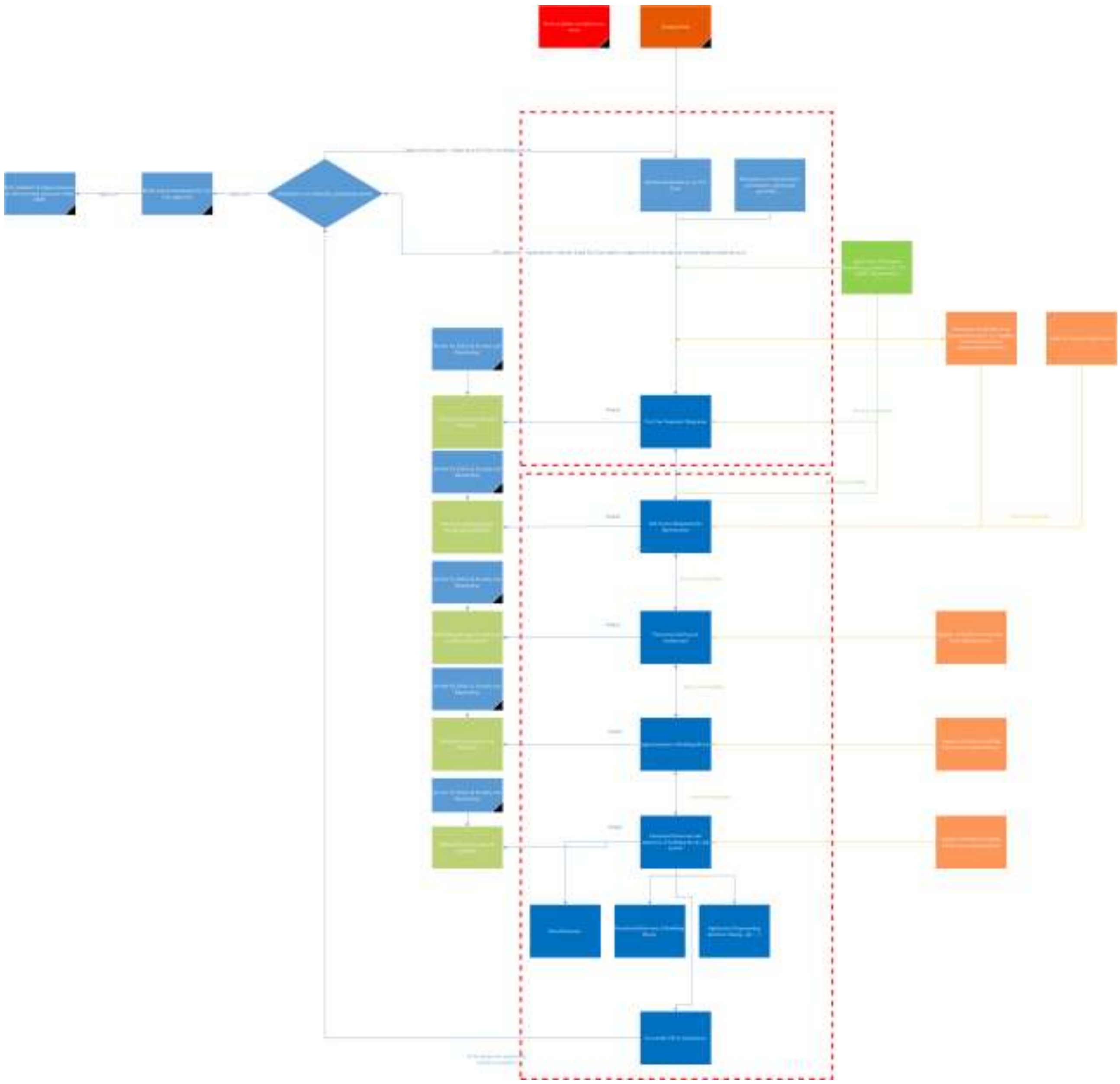

Figure 4: Design Process

Since the EULYNX development process is a representative example of such a development process, it is shown in the following figure 5 as reference.

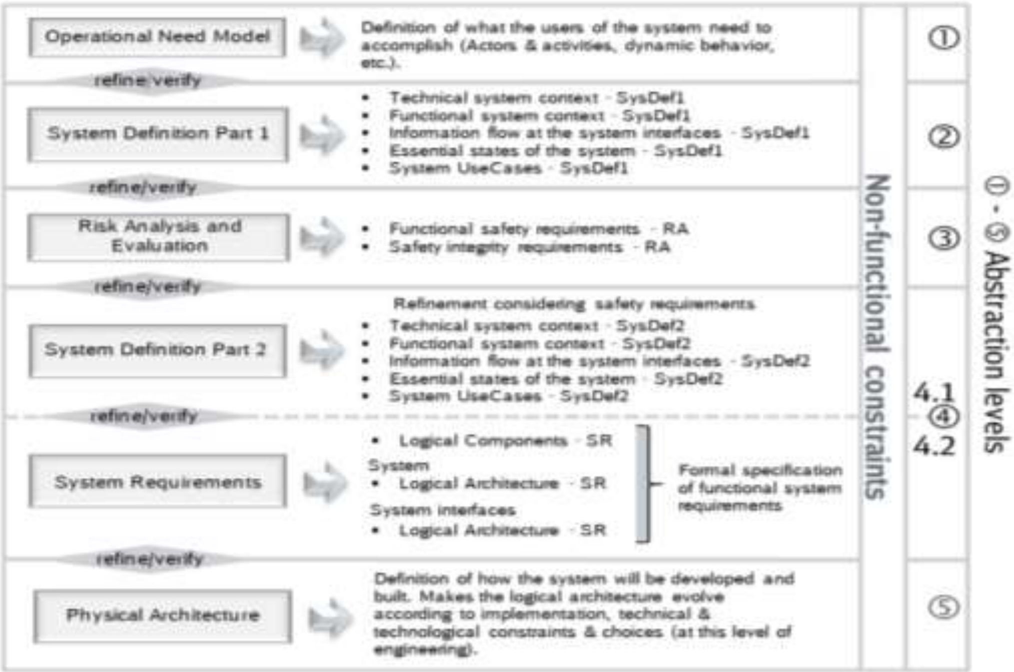

Figure 5: EULYNX Development Process

The following figure 6 provides a detailed view of the modeling toolchain employed in this project. This toolchain has been designed to facilitate the development and validation of the formal model for ATO and RTO systems. It integrates various industry-standard tools and frameworks to manage the entire modeling lifecycle, from requirements specification to implementation and testing. The toolchain was presented in exchange with System Pillar (SP) in 09/23.

Requirements Management with Polarion®

Polarion is an ALM Tool provided by Siemens. Polarion is used as the primary tool for managing and tracing requirements throughout the project. Requirements are meticulously documented in Polarion®, ensuring that each requirement is linked to relevant artifacts within the model. This traceability is crucial for maintaining consistency and simplifying the process of verification and validation.

Sequence Diagrams and Architectural Representations

The modeling toolchain also includes provisions for generating sequence diagrams and architectural representations of the ATO and RTO systems. These diagrams provide a clear and detailed view of the interactions within the system, facilitating better understanding and communication among the project partners. For the presentation of the architecture models, capella is used. Capella is based on the arcadia methodology.

Modeling with SCADE®

Ansys SCADE Suite is a model-based development environment for reliable embedded software, which provides links to requirements management, model-based design, verification, qualifiable/certified code generation capabilities and interoperability with other development tools and platforms." (ansys.com) The central component of our modeling process is SCADE®, a powerful tool for developing safety-critical software. The guidelines for using SCADE are followed strictly to ensure that the generated models adhere to industry standards for safety and reliability. Models in SCADE® are developed based on the requirements specified in Polarion®. SCADE® is chosen since it covers the full lifecycle V-Model of ISO 26262, conforming to EN 50716:2023. The tool chain comprises SCADE Architect®, SCADE Suite®, SCADE RapidPrototyper® and SCADE Display®. SCADE LifeCycle® is used for referencing to Polarion®. The project is set up using the Ansys SCADE® Version 2022R2.

Model Verification and Validation

To ensure the correctness of the models, various verification and validation steps are integrated into the toolchain. These steps include automated checks within SCADE®, peer reviews, and simulations.

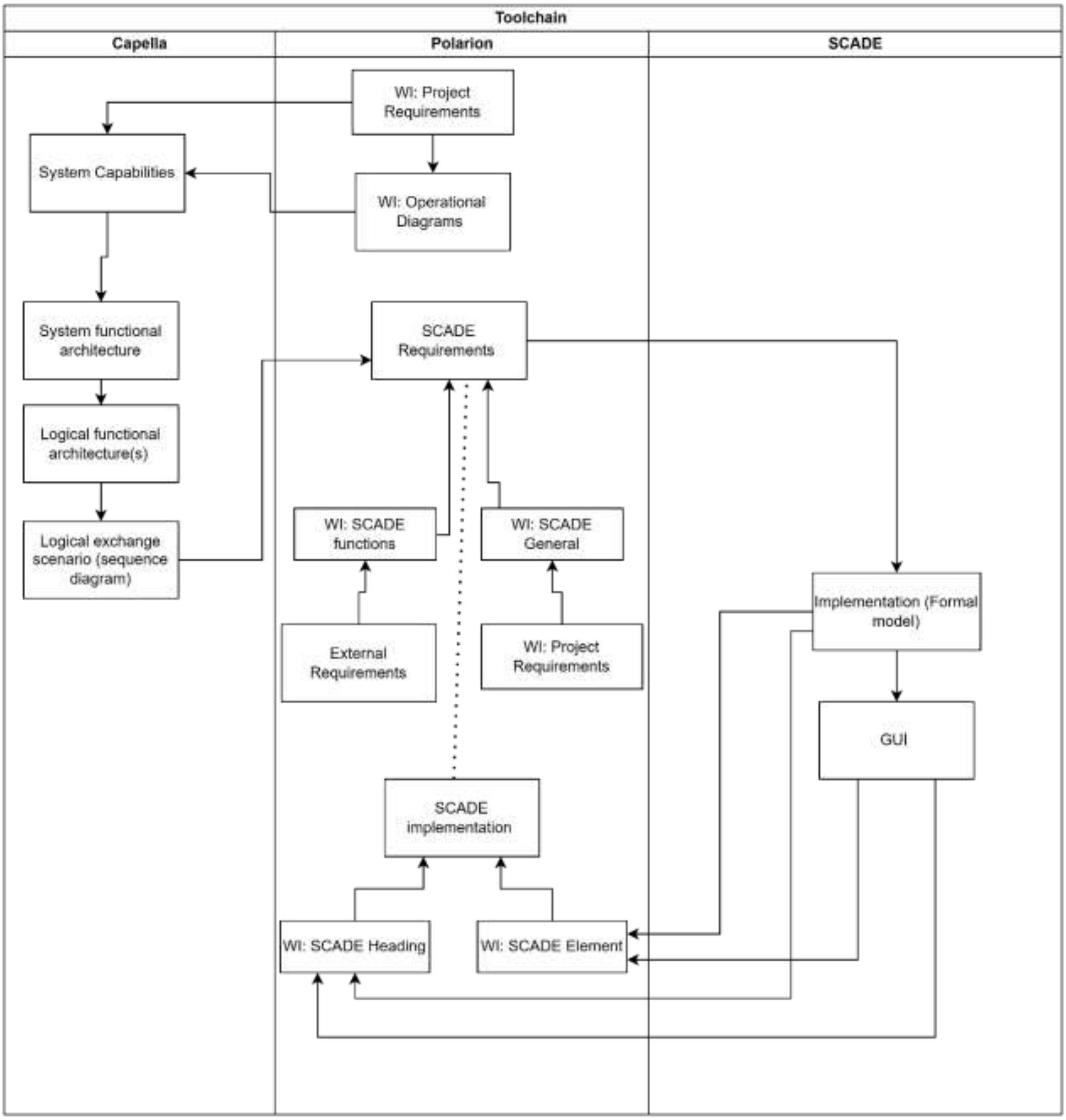

Figure 6: Toolchain Diagram

The exemplary system is modeled following a MBSE method, which is based on the following meta-model. The meta-model establishes relationships between model elements.

Use Case: It refines high-Level Requirements, serving as the primary input for the model, against the backdrop of the (high-level) system definition.

Behavior: Use Cases are detailed through behaviors represented by Sequence or Activity Diagrams. Start and end conditions are annotated, with external actors and entities participating in scenarios.

High-Level Requirement: These requirements are refined by Use Cases, defining operational scenarios and complementing user requirements.

Functionality: Derived from High-Level Requirements, system functionalities are depicted using Internal Block Diagrams that showcase functional interfaces and flows. Functional Analysis describes what the system needs to accomplish—not how it's implemented.

System and Module: Logical architecture is derived from High-Level Requirements to satisfy them, decomposing the system into logical modules. Requiring modularity and interface simplicity, the logical architecture links system functionalities with software or physical architectures. Software architecture within each module comprises interconnected software functions, with granularity varying by module.

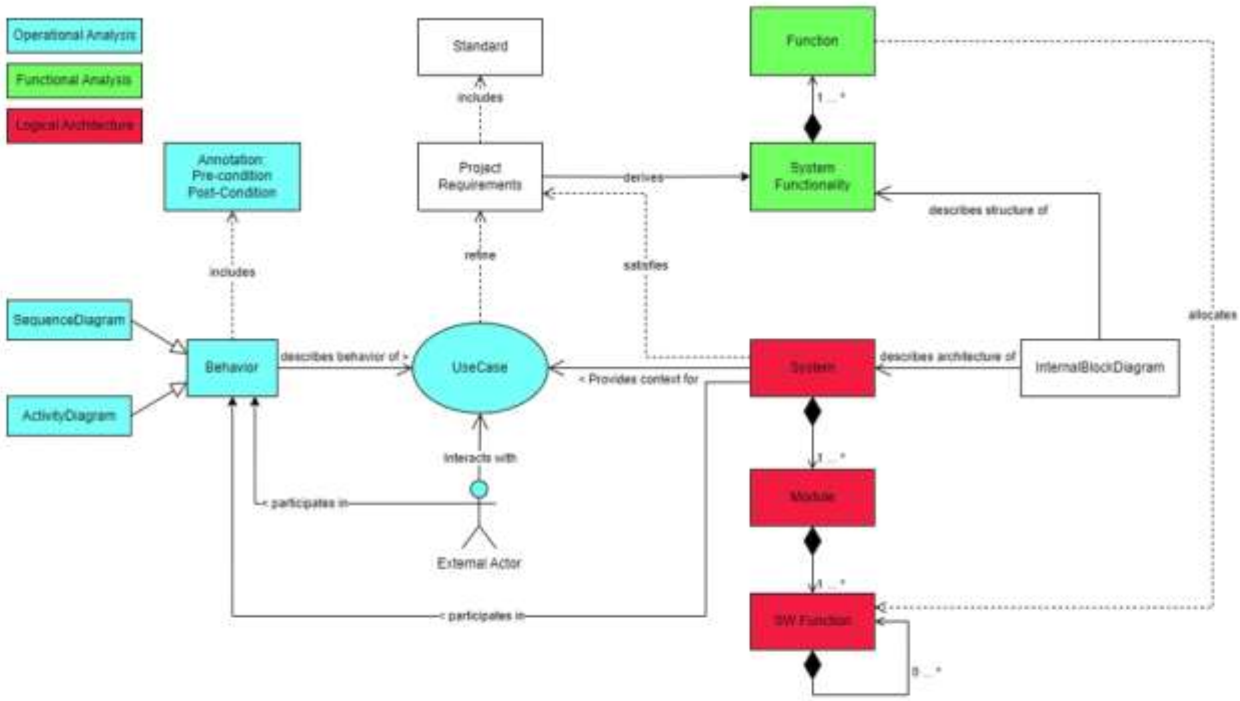

Figure 7: ATO System modeled in SCADE Architect

In the following figure, the Ansys SCADE workflow is shown with the operational analysis corresponding to the blue meta-model elements in Figure 7, while the system design (middle level) corresponds to the green and red meta-model elements. The project requirements contain all requirements on the requirements engineering side, namely user requirements, system requirements, and software requirements.

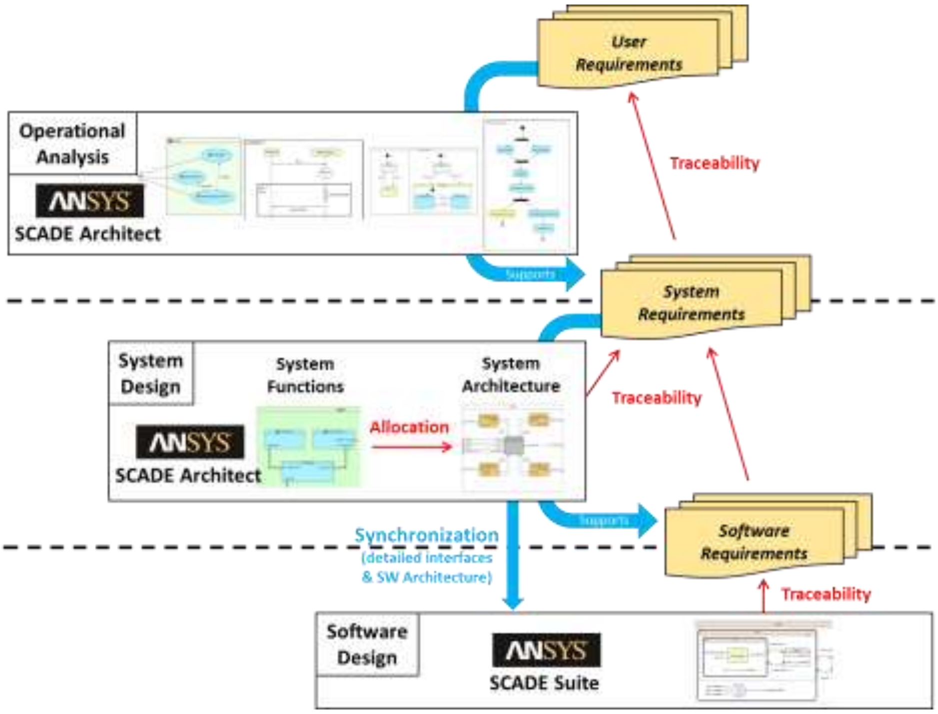

Figure 8: Development workflow

5 SCOPE OF MODELING

In this chapter, the modeled use cases are presented for scope definition. The mentioned examples serve as examples to demonstrate the modeling processes. These are not technological results. The following definition of RTO is a first necessary step to clarify the different scopes of RTO in the FP2-R2DATO context. The definition needs to be seen as a first suggestion for further discussion. It is not aligned neither with other WP in FP2 nor with the "ATO-Cargo" project consortium.

5.1 ATO GoA4 AND RTO GoA4

The ATO and RSC mainline use case focuses on freight operation on the mainline operations under ETCS full supervision (FS). Accordingly, shunting yards are out of scope. Requirements represent the development of (partial) GoA4 operations with Full GoA2 and selected GoA4 functionalities. Remote Supervision and Control (RSC) was designed for the supervision in GoA4 mode and remote control in degraded mode. For more details, please refer to the operational sequence diagrams in the results section as well as to D5.5 [3] for more details, e.g. on actors and systems. In the following, the naming RTO (Remote Train Operation) is used instead of RSC in accordance with the naming aligned in System Pillar. RSC Mainline is the term used in the Grant Agreement.

5.2 DEFINITION OF RTO

Currently, RTO is used in many ways without their clear definition.

Basically, an RTO is understood in two ways:

a) RTO as a backup for degraded mode of ATO, usually ATO-GoA4.

b) RTO as operating mode for use in unmonitored areas in shunting and parking areas.

Therefore, a definition of RTO according to different modes is essential. A clearer (basic) distinction can be made according to the different ATO Grade of Automation modes (for an application of this concept within FP2-R2DATO, see also deliverables of WP38, especially D38.2 [7] and D38.3 [8]). However, even with a defined RTO use of a specific ATO GoA mode, further differences may exist.

An RTO definition is supplemented by the boundary conditions of a specific operation (specific functional requirements of the individual RUs). This is particularly evident in the functionalities in a degraded mode, e.g. limited monitoring or limited remote control operation by a remote operation center, up to and including completely autonomous fault self-healing.

The extent to which visual sensors can be separated from a perception system (for ATO GoA3/4 use) must be further investigated in terms of reliability, availability and safety quality (SIL requirement) as well as an APM system with reduced functionality (obstacle detection without object classification) and safety requirements (SIL-Zero or No-SIL).

For the use of RTO as extended ATO functionality, e.g. GoA2, or for a degraded mode under a functioning, fully monitored ATP system, the system interfaces to ATP/TCMS and data communication must also be examined in detail.

Definition

Remote Train Operation (RTO) is a technology letting operators control trains from a distance, not physically in the cab, using tablets or controllers for tasks like yard shunting or as a fallback for automated systems, enhancing efficiency and safety by reducing human error in hazardous situations, and leveraging cameras/sensors for situational awareness, with systems designed to stop the train automatically if communication fails.

How it Works:

- Control Unit: Operators use handheld devices or computer interfaces to send commands (accelerate, brake).
- Connectivity: Relies on advanced, often secure, communication networks (like 5G) for real-time data.
- Sensors & Cameras: Live video feeds and object detection help operators observe the train's surroundings.
- Fail-Safe Design: Systems are built to automatically apply emergency brakes if communication is lost or the controller is misused (e.g., tilted too far).

Key Applications:

- Rail Yards: Most common use for assembling trains and moving cars, improving safety in complex environments.
- Depot Operations: Maneuvering trains for maintenance or stabling (standby).
- Main Lines (Emerging): Acts as a backup or assistance tool for automated mainline trains, allowing remote driving for disruptions or emergencies.

Benefits:

- Safety: Reduces accidents from human error, especially in tight spaces or poor visibility.
- Efficiency: Improves productivity, deployment, and flexibility in yard/depot management.
- Situational Awareness: Cameras provide a clear view, and hazard detection aids decision-making.
- Labor: Addresses skilled labor shortages and optimizes crew deployment.

Similar to the Grades of Automation (GoA) defined for ATO, different levels of RTO can also be distinguished. This is important, since the different levels of automation for RTO have important aspects on the necessary system design (see also chapter 6.4). This is summarized in the following diagram (see Figure 9).

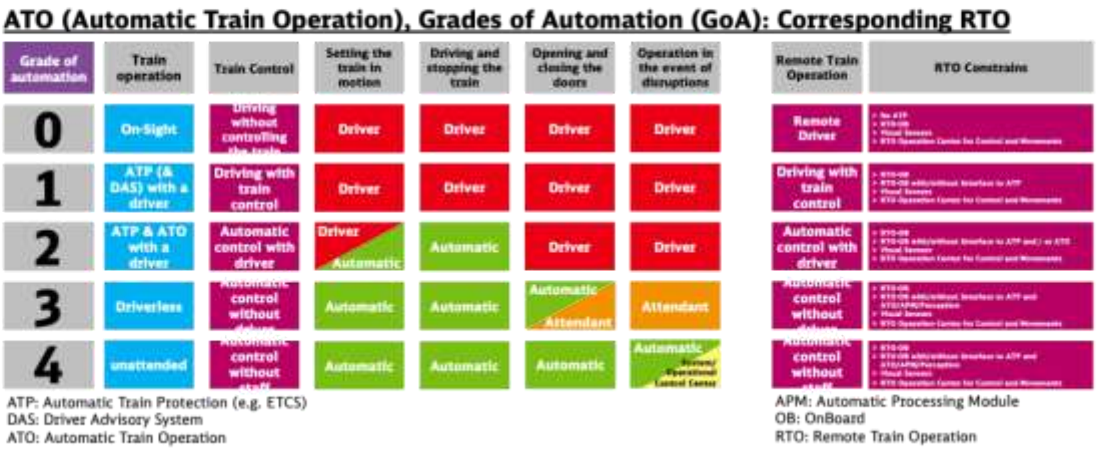

Figure 9: RTO Definition. Using different grades of automation, analogous to ATO.

5.3 YARD TO STATION MOVEMENT

This deliverable presents the context of MBSE for modeling freight specific use cases (ATO mainline and RTO). Within the work package (WP31), another approach uses MBSE for another use case. The according use cases, focusing on passenger trains for yard to station movement can be found in deliverables D31.4 [9] and D31.5 [10] of FP2-R2DATO.

6 MBSE APPLICATION EXAMPLE

As described in the design process, the different steps are shown in the following as exemplary application of the models. However, their character is only exemplary and not to be understood as a technical contribution. More specifically, the processes shown give an example for the modeling of processes but are not validated and need to be aligned and reworked by technical and operational experts to represent technical results. Further developments are ongoing.

6.1 Operational Diagrams (Exemplary)

This chapter details operational processes related to the ATO and RTO mainline use case. The processes are described through a series of "Contextual Capability" diagrams and "Entity Scenario" diagrams (sequence diagrams). These diagrams are created using the modeling tool "Capella". The contextual capability diagrams show which external system actors are involved in each individual use case. The sequence diagrams show how the external actors and the system of interest interact with each other.

Actor	Description
Train Driver	A person capable and authorised to drive trains, including locomotives, shunting locomotives, work trains, maintenance railway vehicles or trains for the carriage of passengers or goods by rail in an autonomous, responsible, and safe manner.
RTO Operator	A person responsible for monitoring a single train's operation and capable of remotely driving the train.
RTO Supervisor	A person to monitor the high-level status of ATO / RTO trains. This person is triaging issues with an ATO GoA 4 train and can allocate this train to an RTO Operator.
Rolling Stock Operation System	The Rolling Stock Operation System represents a collection of functionalities of on-board systems which are external to the system of interest. This includes the Train Control Management System and other control systems, e.g, door control, traction control, or braking control, and can be specific to the class from the supplier of the rolling stock; but it interacts with the system of interest over standardized interfaces.

Table 2: Actors in the exemplary operational scenario.

The following actor overview shows the actions of the actors train driver, RTO operator and RTO supervisor for transitioning actions as a starting point of the further modeling. The defined processes hereof are presented in the next subchapter in written text.

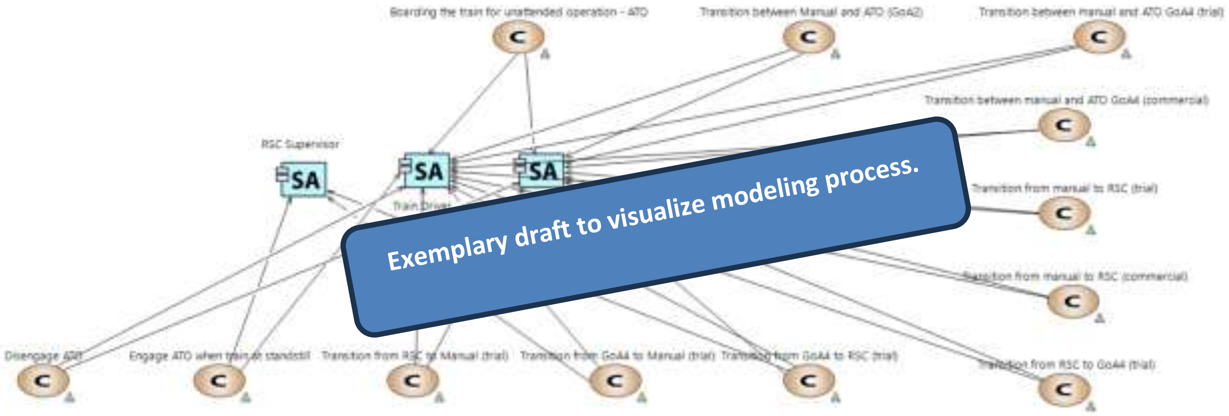

Figure 10: Overview of transitioning activities for the involved actors Train Driver, RTO Operator and RTO Supervisor.

In the following subchapters, key use cases with a focus on freight specific applications are presented as exemplary cases for automatic driving.

6.1.1 Train driver boarding an automatic train for manual operation

This use case details the interactions of the train driver, RTO supervisor, and RTO operator with the system to allow the train driver to board an automatic train for manual operation.

Preconditions:

- Train at standstill
- Train in ATO or RTO control
- External Override Switch deactivated

Postconditions:

- Train driver onboard
- Train is in a manual state

In the following, the Actor view as well as the sequence diagram are shown for the use case “Train driver boarding automatic train for manual operation”.

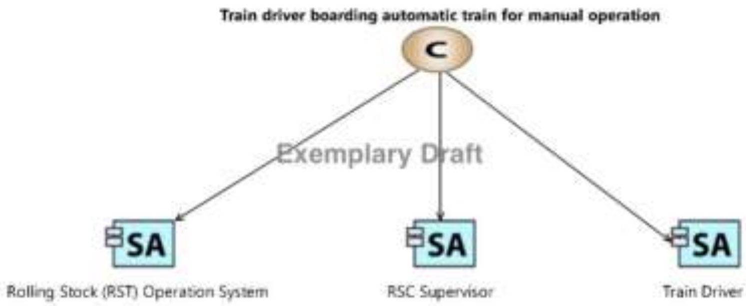

Figure 11: Actor view (Train driver boarding automatic train for manual operation).

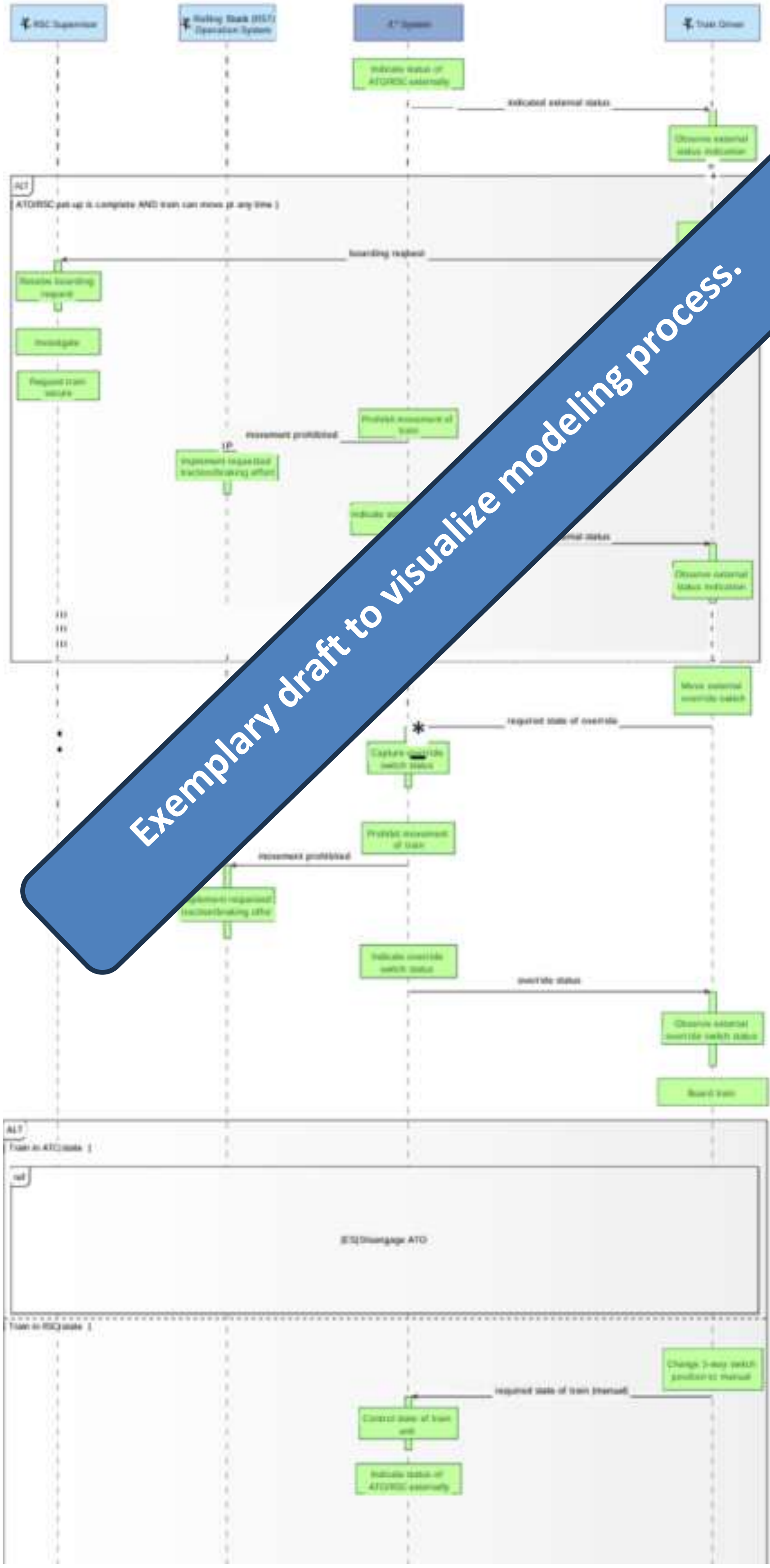

Figure 12: Sequence Diagram (Train driver boarding automatic train for manual operation).

6.1.2 Train driver boarding manual train for automated operation

This use case details the interaction between the RTO supervisor and the train driver with the system to allow the driver to board a manual train with the goal of setting up the train for GoA4 operation.

Preconditions:

- All locomotive systems initialized;
- ETCS localisation is available
- ATO/RTO inactive;
- Mode switch in manual
- External Override Switch deactivated

Postconditions:

- ATO in control of train

In the following, the Actor view as well as the sequence diagram are shown for the use case “Train driver boarding automatic train for automatic operation”.

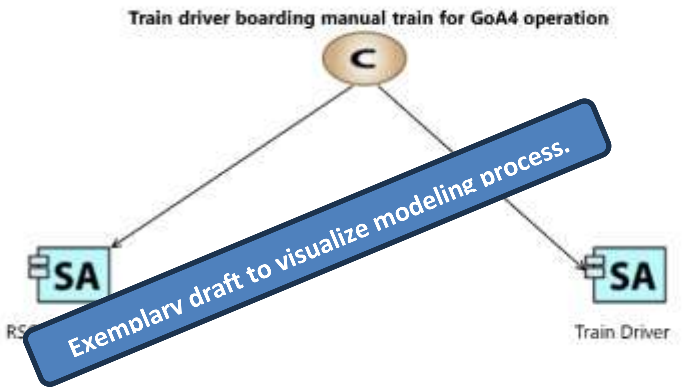

Figure 13: Actor view: Train driver boarding automatic train for automatic operation.

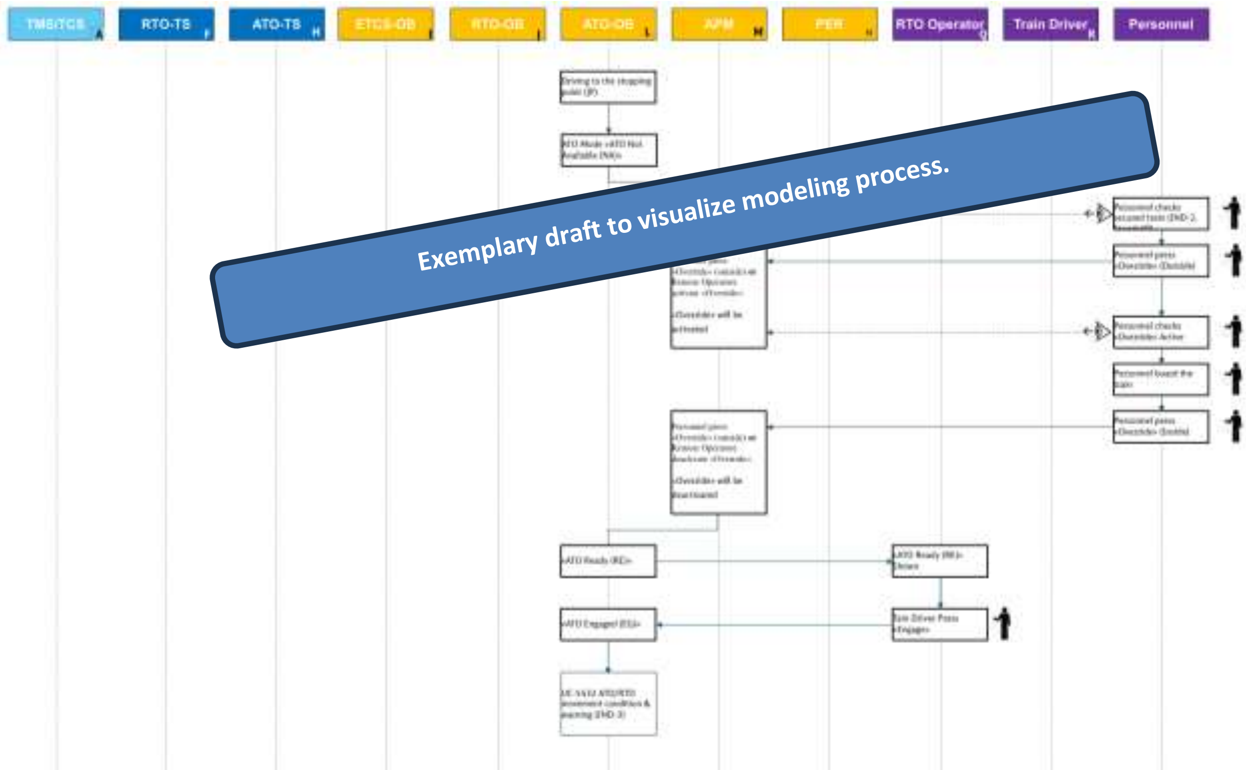

Figure 14: Sequence Diagram: Train driver boarding automatic train for automatic operation.

6.2 RTO SEQUENCE DIAGRAMS

The following sequence diagrams illustrate some of potential behaviors of the RTO system. In particular, they describe sequences of events. For future applications, especially control transitions and data transfer between the trackside systems and the rolling stock need further development.

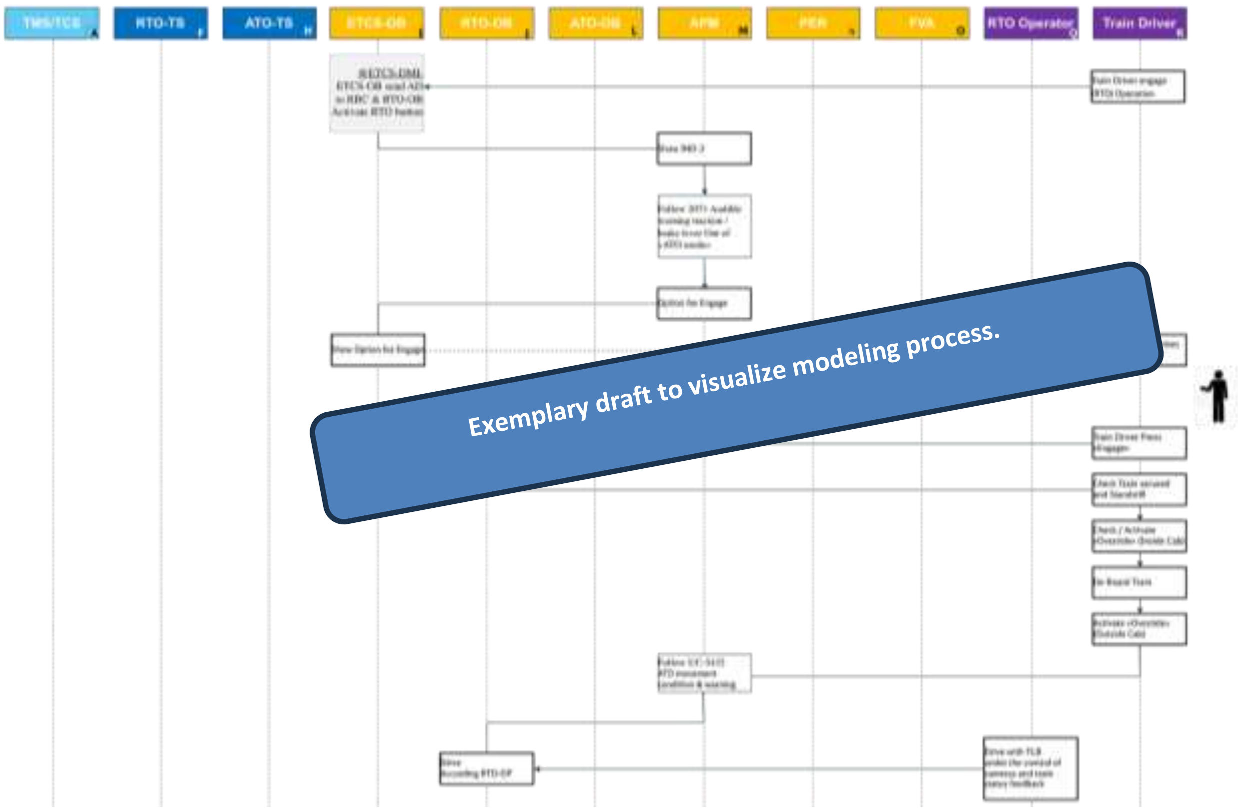

Figure 15: Sequence Diagram: Transition Manual Driving <> RTO.

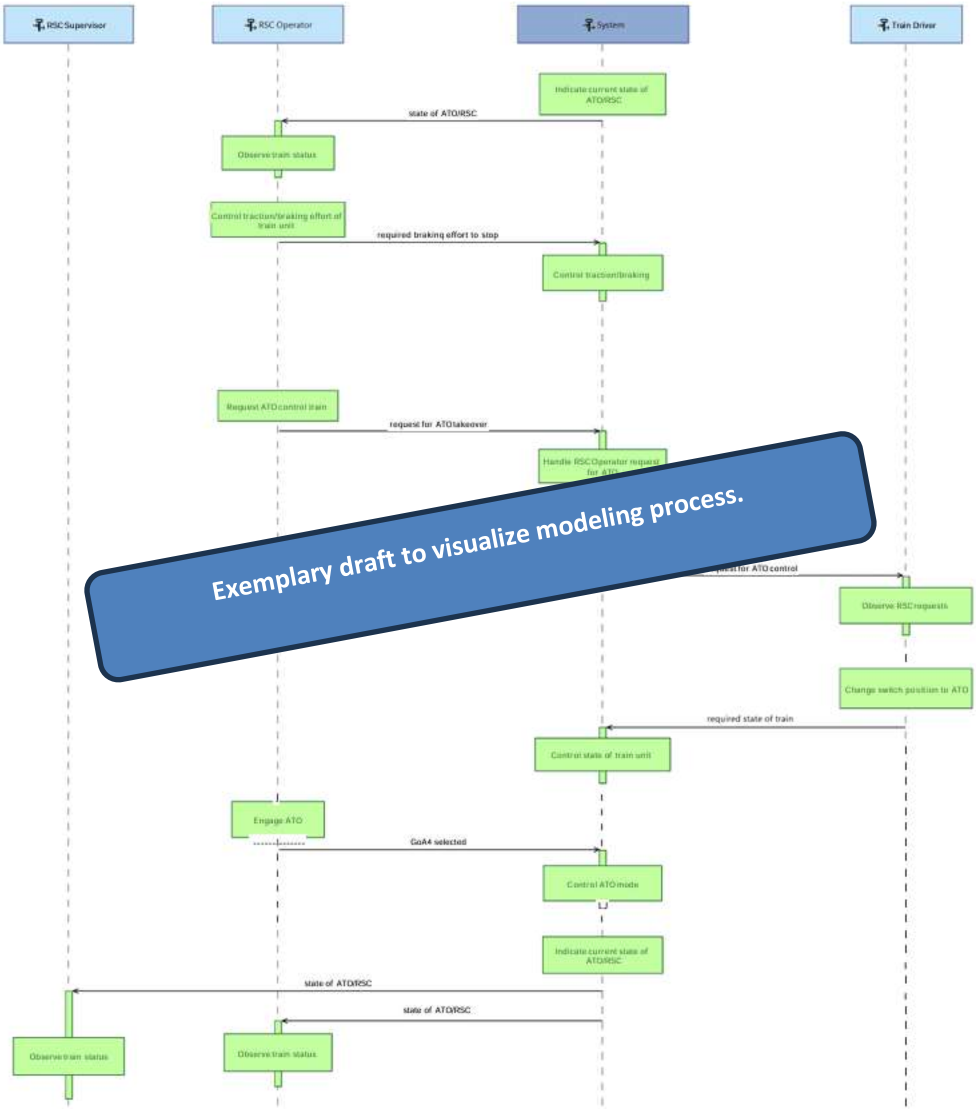

Figure 16: Sequence Diagram: Transition RTO to ATO GoA4.

A state machine allows for correctly modeling state transitions as shown in the simplified GoA2 state machine in the following figure. The following exemplary draft shows ATO engaging. It supports finding missing interfaces and information. For example, the movement warning for the locomotive needs to be addressed, also in existing specifications. In addition, icons for the different use cases (ATO, RTO, levels of automation) need to be defined.

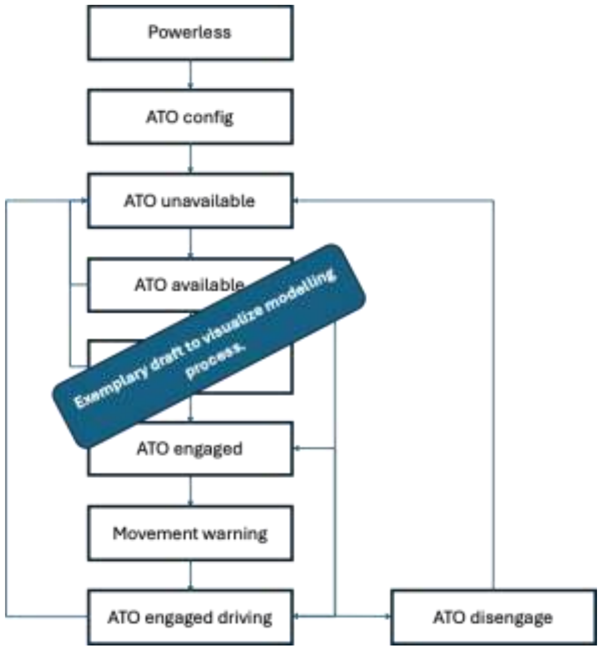

Figure 17: ATO-OB / ADM state machine example

6.3 DMI GUI MODELING

As an example of the MBSE workstream, the simulation of the DMI for ATO driving in GoA4 including the interfaces and the necessary interactions was produced. It is a basic mockup that needs expert revision and does not contribute as technical result. It is shortly described in the following.

The simulated DMI is a basic mockup for the ATO-specific information needed. This also applies to the ETCS TS. The GUI of the DMI is shown in the following figure.

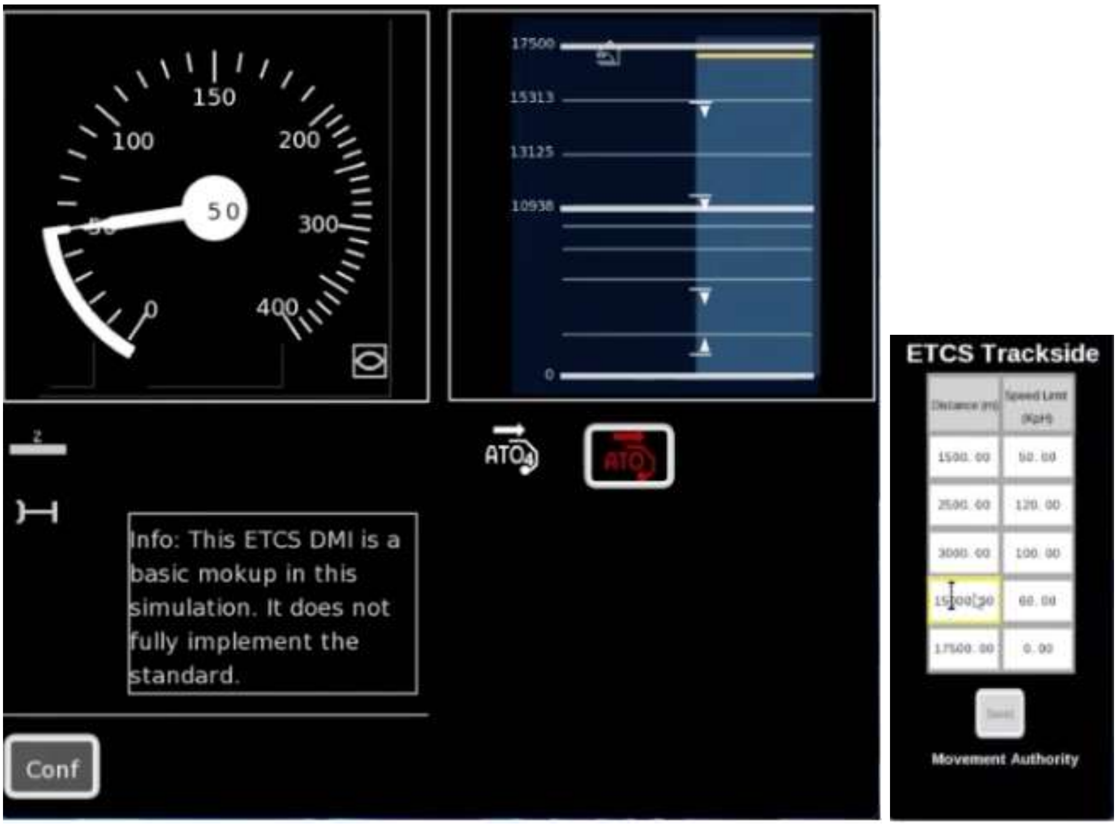

Figure 18: GUI for the rolling stock controls.

These controls simulate the physical controls on the locomotive and shows the simulated train speed.

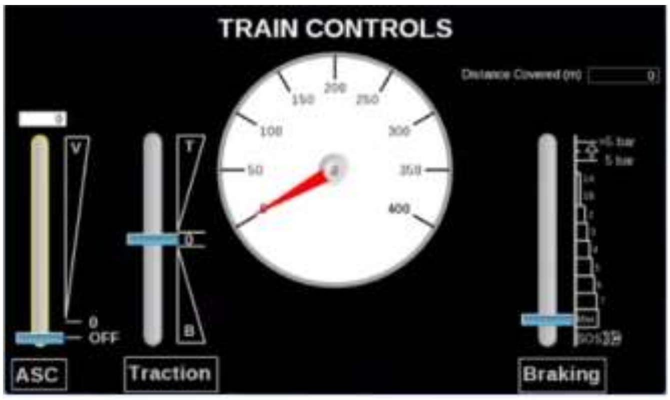

Figure 19: GUI for train controls.

The diagnostics GUI that details the internal states of the simulation and its architecture components, is shown in the following.

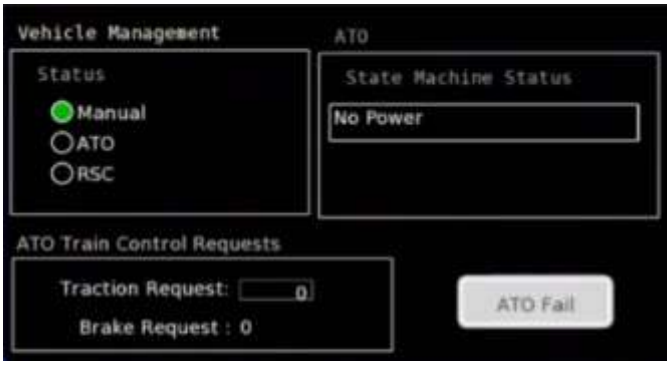

Figure 20: Diagnostics GUI.

Finally, additional switches, buttons and lights are proposed as part of the research outcome, as shown in the next figure.

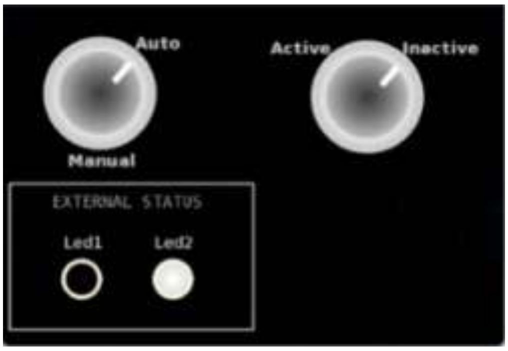

Figure 21: Proposed additional switches, buttons and lights.

The modeled GUI revealed the need for further research for the design of the icons indicating the current mode, e.g. the need for “RTO” indication to be easily distinguishable from an “ATO” mode, especially in the remote driving context.

6.4 Modeled Architectures

The freight specific architecture, the modeling was based upon, is presented in FP2-R2DATO D5.5 [3]. Further developments are ongoing and further adaptations of the architecture in [3] are necessary.

With regard to the architecture, is important to distinguish different designs for different levels of RTO, analogously to ATO via different levels of automation (GoA) (see chapter 5.2). Especially interfaces of the RTO-OB may imply that the technical solution of the RTO needs to be different for different levels of RTO due to e.g. the absence of other systems, such as the APM for e.g. GoA0 (or GoA1 analogously).

For the architectures developed in OCORA (CCS-OB, Train Adapter, a.o.), please refer to [13].

Further developments are ongoing.

6.5 WP6 Gap analysis

In this document, the methodology of MBSE is presented to model freight specific use cases. By doing so, technical elements are described that are the basis for modeling. However, since freight specifics are hardly touched in other contexts of FP2-R2DATO, the following chapter presents a gap analysis of the systems with the specifications developed in WP6 of R2DATO. The analysis is done for D6.5 [11] and D6.8 [12].

The reviewed documents [11, 12] are extensive and, very detailed with respect to some specific aspects. In general, the gap analysis for freight aspects reveals the following aspects:

- Freight specific topics are hardly touched.
  Examples: train configuration for driving profile calculation, there is no movement warning (see chapter 3), no outside visual identification of an unattended train, boarding deboarding process.
- The use of passenger or freight locomotive-hauled trains (including those with multiple and/or distributed locomotives) is not dealt with, except for a few minor points.
- The topic of RTO is not systematically addressed. It is used in different contexts (for different GoA levels) and used selectively, for different remote applications with different degrees of automation. The description of interfaces, operational scenarios, handshakes or modules can be further detailed.

6.5.1 R2DATO FP2 D6.5

The following aspects were identified in the gap analysis for D6.5 [11]. The analysis has been made after finalizing the freight modeling for this document when D6.5 was already finalized. It should be noted that the following aspects focus on the gap analysis from a rail freight perspective.

<u>General findings:</u>

- There is a need for a general definition of Remote Train Operation (definition, functions, use case, interfaces, logical and physical architecture, modules, operational processes, responsibilities of human and legal entities, …) according to the different operational contexts (8.1.1.1.1).
- Corresponding Table 8.1 “Operating contexts”, Section 8.2 Figure 1 “Train Context State” and Figure 2 “Operating Context State Diagram for Trains“ shall be further elaborated for RTO modes and responsibilities in the future. It is essential to consider the difference between supervision and operator, as well as their infrastructure (RTO desk).
- GSM-R (Area) emergency stop call, function, interface and detail operation process is missing.
- 7.10.3.1.2 The local remote-control definition is missing. The term is misleading; it probably refers to a train recovery technician/driver in the train-cab.
- 7.10.3.1.2 “local remote control” vs 7.10.3.1.3 “local staff” is unclear and missing in the terms.
- RTO restrictions (failure or reduced functionalities, e.g. disruptions / reduced perception) must be indicated within transmission of possible automation mode GoA3/GoA4 to trackside and the mode selection.

- 8.2.1.1.5: "The responsibility for the train as such, i.e., to keep brakes applied sufficiently, is still with the TCMS and the physical train". Change to TCMS AND/OR physical train
- Incidents detected by driver (additional section as 8.5.1.1.8 for TCMS) is missing. A driver can detect anomalies that arise in the interaction between different systems, even if the individual systems do not report any errors.

What needs to be aligned for freight use cases

- Rules presume a driver in the cab. Operational scope ties to ETCS up to system version 2.2, with the rulebook written around driver actions on the ETCS DMI with unattended concepts being not addressed.
- Voice procedures and European Instructions require signaller - driver exchanges (e.g., authorising start in SR, passing an EOA),3.3. Terms needing further alignment/ precision:
  - Definition of remote driver. RTO-Supervisor and RTO-Operator work based on primary functional task responsibilities. Awareness, task workload and education / experience must be considered.
  - Freight Customer (11.7) definition is missing. Freight RU or wagon holder, owner must be defined
  - Holding brake is not explained or specified
- 6.3.1.1.4: Still ATO-OB (of TSI 2023) isn't sufficiently specified for GoA2 (and later GoA4) and must consider freight-specific functionalities (e.g. different brake-Systems) to increase operation performances (reducing the operational headway), to reduce operation cost by saving energy consumption and to enhance the punctuality and to reduce the mean journey time.
- 7.3.2.1.9 Train data (details of length and weight, type of wagon for cargo or coach…) is required for a freight operation (journey or a mission).
- 7.3.2.1.11 Train Data will be needed for any journey calculation and will be also available for the IM-Server.
- 7.10.2.1.7 RTO Operation cannot be shared between RU and IM. Owner / Operator is legally responsible for traction / brake within a IM protected area (MA).
- 8.6.3.2 APM GoA4 Operating Conditions: GoA3 and GoA4 need an additional condition of an available and functioning RTO operation.
- Table 8.5 – Transition conditions table (APM): Transition table must be extended by RTO issues (availability and RTO operational needs) 9.4 Emergency manager: Person of the Infrastructure legal entity could not directly or remote operate a train. In case of an emergency an emergency intervention group must be initiated with persons of the different entities (Infrastructure and RU) as well as from blue-light organizations.
- 9.16 Train Control and Monitoring System: TCMS does not control (definition of control is missing), TCMS is managing subsystem.

- 10.2 Automatic Driving Module: ADM functionalities to be assessed for further functions, as different brake systems or pantograph (Raise, lower and switch from country specific pantographs)
- 10.3 Automatic Processing Module: APM functionalities to be assessed for further control / manage functions (e.g. movement warnings and indications)
- 11.14.1 Indicate the presence of the vehicle to others: update with freight specific locomotive movement warning
- 11.14.4 Provide Brake Command for Parking Braking: Changes and extension for locomotive and freight trains needed.
- 11.14.6 Provide Brake Command for Service Braking
11.14.7 Provide Brake Command for Holding Braking
11.14.8 Acquire realised braking effort
needs to be reassessed for the different freight brake system.
- 11.16.1 Manage energy supply for traction. Train protection do not know the layout of train locomotives and wagons.
- 11.16.24 Provide juridical data recording: Recording time for video material (ring buffer of 1h for example) needs to be updated according to country specific requirements for (maximum) recording length and automated delete of recorded streams.
- 11.17.1 Couple locomotive: Description must be updated if train consist of two or multiple locomotives.
- 12.2.3 Respect JP Timing Points and Optimize the consumption: ATO-OB must take into account the requirements when calculating the speed profile of freight driving rules and limitations (see chapter 3.1)
- 12.2.6 Acquire train and ADM data: Train configurations and individual detail information of each involved locomotive characteristic is needed.
- 12.10.1 Manage trackside incidents: Trackside Incidents shall be detected also by a trackside perception system.
- 12.10.2 Manage train incidents: Any train incidents shall initiate an Alarm and send to the RTO-Supervisor.
- 12.18.7 (TUM-7.4) Process remote driving commands: RTO Operation shall be available in ETCS FS. RTO operation will be activated at degraded ATO-GoA4 Mode, regardless of the ETCS mode.
- 13.4.5 Cut current, lower and change pantograph: Main circuit breaker and pantograph are controlled by Train Protection with track conditions during train run. Train Protection does not know the train configuration and therefore may not be able to trigger a timely action based on the balise information.
- 13.7.6 Move the train locally: Local control of a train by trackside staff is not useful. It must be a trained and certified specialist from an RU or special rescue team.

What needs to be specified for freight use case ATO GoA4 and RTO mainline, compared to D6.5

- Remote supervision and control requirements, architecture (influence), modules and operational processes. (e.g. RTO-OB in Section 7.x)
  7.10.2 exports some constraints to TCMS (e.g. speed control). TCMS does not have a maximum speed based on the route or train configuration. RTO Supervision and Control responsible and desk definitions is missing.
  RTO and ETCS interfaces (Onboard as well as trackside) must be defined, and special RTO Mode must be included within ETCS specification.
  RTO needs to be analysed in detail by functions, use cases, requirements, logical and physical architecture module and corresponding interfaces.

- Remote supervision and control model. Who replaces the driver for European Instruction flows? How remote operators are authenticated and logged is not specified.
- Remote recovery/degraded-mode procedures (e.g., after trip, level transitions, or SR running) without a driver. The listed rules describe driver actions.
- Perception Trackside and direct interface from/to Perception (Onboard) is missing in “6 System Scope / 6.1 Overview” and “Figure 6.1 – Logical Architecture”
- Constraints to Remote supervision and control Zones (7.4.2) is missing.
- The RTO supervisor and RTO operator to be defined (not described in “9. Description of the actors”).
- RTO Module and all interfaces to onboard modules as well as communication to RTO trackside to be defined (not described in “10 Description of logical components”)
- Interface from PER to Perception trackside to be defined (not in “10.4 Perception”)
- 10.14 Train data is necessary for freight operation in GoA2 and GoA4 and could not be outside of scope GoA3/4.
- 11.2.8 Drive train remotely is needed for a stable GoA3/4 operation. Requirements, use cases, logical and physical architecture, module specification, interfaces as well as operation constrains and actors must be defined. Within 10.2.8 Drive train remotely the need of an independent camera system could not be handled as exported constraint. A corresponding trade-off is needed considered availability and reliability of perception and perception sensors/cameras.
- “11.9 Light signal” constraint for GoA3 / GoA4 operation to be added.
- 1.14.27 Provide train radio information: This function manages the train radio information when this device is present. It changes the channel of the voice radio communication system when requested and sends train radio alarm. The function provides the status of the track-to-train radio. An anomaly must be known by the system because it is used by driver to communicate an emergency order (not necessary in GoA4).
- 11.14.31 Provide Test (Emergency Brake) needs to be reassessed for different brake systems.
- 11.14.32 Acquire brake demand (direct brake) needs to be reassessed for different brake systems.

- 11.14.33 Configure brake system needs to be reassessed for different brake systems.
- 12.2 Automatic Driving Module: Speed profile calculation must consider "Non-Stopping sections" and prevent brake overheating.
- 12.2.2 Determine maximum authorised speed: Train configuration must be considered (e.g. multiple locomotive).
- 12.2.7 Regulate traction and braking effort: powerless and power change sections must be considered. In addition, overheating of the brakes must be avoided.
- 12.8.1 Record on-board data: In degraded mode RTO will be active and ORD shall record RTO-OB data (e.g. speed, …).
- 12.18.8 Provide video: analysis for RTO cameras to be independent from PER needed in future (availability and reliability of the GoA3/4 systems, like PER, cameras, APM).
- 13.4.3 Test brakes dynamically: Test before downhill as brake de-icing shall be specified. If the brake failure RTO Supervisor shall be informed by an alarm message.
- 13.8.11 Manage adhesion problems: Adhesion management is a key function for a freight operation and is missing.
- 13.12 System failure scenarios: Rescue and Technical support teams to be specified in the future.
- 13.13 Transition: All transitions from GoA2/3/4 operated train to RTO, Rescue and Technical support teams to be specified in the future.

6.5.2 FP2-R2DATO D6.8

Freight context of RTO:

Remote Train Operation (RTO) is a key component of the GoA4 operational framework, supporting the safe and efficient deployment of unstaffed freight trains. It provides the central interface for monitoring, supervision, and—when required—remote control of trains operating in ATO mode. RTO interacts continuously with both onboard and trackside RTO elements to ensure real-time data exchange and maintain authority over train configuration.

What needs to be aligned for freight use cases ATO GoA4 and RTO mainline

- There are naming differences that need to be aligned in the future. Here, RTO naming was used in accordance with System Pillar naming.

  Exemplary naming. The second term is used in this context.

  - Control-On-Board (RC-OB) <> RTO-OB
    Remote Control Centre <> RTO Center
    Remote Cabin <> Remote Desk
    Remote Control-Trackside (RC-TS) <> RTO-TS
    Remote Supervision Centre <> RTO Center
  - “Command brakes” is not specific enough for freight application. A distinction may be needed between electro-dynamic brake (EDB), pneumatic train brake and locomotive brake
- Apply brake command: When this function is performed, the train applies its brake, as specified by a brake percentage. For all braking applications, all different braking solutions, electrodynamic brakes (EDB)/pneumatic train brakes/locomotive brakes, must be taken into account. Raise or lower pantograph (optional): This function is not optional, as the control (timing) of the pantograph(s) must be calculated and executed according to the train configuration (mission profile) and the corresponding speed.

OPE rules are only declared applicable up to ETCS OB system version 2.2. Today’s operational rulebook is framed around current ETCS baselines with a driver.

What needs to be specified for freight use case ATO GoA4 and RTO mainline, compared to D6.8

- RTO Specification (Architecture variants and corresponding Interfaces)
- (independent of ETCS-ATO, SS130) interfaces ETCS and RTO-Onboard
- Overall architecture and handshake as well as fail-safe interfaces between different modes and the different Onboard (sub) systems (ETCS – ATO – RTO)
- No detail specification of Remote Supervisor exists as well as handshake between RTO-supervisor / RTO-operator handover.
- Outside indications for locomotive mode and movement warning
- Handover from an RTO Supervisor to an RTO Operator
- Extension of DMI icons for GoA4 and RTO Operation mode.
- GSM-R (Area) emergency stop call: Function, interface and detail operation process from RTO-Operator to CAB-Radio

7 CONCLUSION AND RECOMMENDATIONS

A central conclusion is that freight automation introduces fundamentally different operational and technical requirements compared to passenger contexts. Freight trains exhibit distinct dynamic characteristics, braking behavior, train consist variability, and operational risks. These factors, highlighted throughout this deliverable, necessitate a tailored methodological approach that integrates freight-specific behaviors into the formal models from the outset. The MBSE workflow applied in this task proved capable of capturing such complexities, particularly through the use of sequence diagrams, architectural decomposition, and functional allocation. This ensures that use-case-driven insights translate directly into system design and interface requirements.

A second major conclusion relates to the regulatory environment. Current TSI OPE, TSI CCS, and UNISIG Subsets remain insufficient to support unattended GoA4 freight operations or RTO. Existing specifications assume a human driver onboard, rely on driver-mediated degraded mode handling, and do not define processes, interfaces, or safety responsibilities for remote supervision or remote control. As a result, many operational procedures lack a regulatory foundation. The modeling work in this deliverable illustrates concretely how these gaps influence system behavior, operational feasibility, and safety allocation.

Third, ATO and RTO cannot be viewed as independent extensions of existing ETCS or TCMS functions. Instead, they form a tightly integrated system-of-systems that requires clear functional boundaries, defined responsibilities, and robust communication interfaces. The modeling activities confirm that these modules can be formally represented and interfaced—but only if new standards define their role, safety contribution, and data requirements. In this regard, the modeling process improves transparency and provides a structured foundation for future standardisation.

Finally, the work shows that formal modeling not only supports technical clarity but also provides concrete operational value. Through the depiction of procedures such as boarding/deboarding, ATO engagement, RTO control transitions, the models help operators, infrastructure managers, and system suppliers gain a precise understanding of workflows that would otherwise remain ambiguous in purely textual specifications. This directly supports safety argumentation, test preparation, and system validation.

Based on the findings of this deliverable, the following recommendations are proposed:

- Advance harmonised European specifications for GoA4 freight and RTO. ERA, UNISIG, and EU-RAIL should jointly develop formal definitions, procedures, and interfaces for RTO roles, remote degraded-mode handling, and unattended GoA4 operations.
- Establish a structured MBSE-based standardisation method. Future specifications should incorporate a formal modeling layer, not only text, to ensure unambiguous interpretation and to increase the consistency of system and subsystem requirements.
- Extend ETCS/ATO frameworks to support unattended operation.
- Integrate freight-specific dynamics into future system designs.
- Develop reference implementations and demonstrators. A standardised demonstrator architecture, executable via standardised tools, should be established to validate the formal models and provide a reusable foundation for industry and suppliers, since current European-level discussion still claim non-standardised tools to be used in MBSE toolchain.

REFERENCES

[1] Shift2Rail - IP5 - ARCC Demonstrator – Deliverable 1.7 "Documentation and evaluation of GoA2 freight demonstrator test results in specified testing scenarios, proposal of next steps".

[2] OCORA Open CCS On-board Reference Architecture, 2020. High Level Methodology, Gamma Release. Document ID: OCORA-30-006-Gamma. Version: 1.10. Document ID: OCORA-30-006-Gamma. Available online: https://github.com/OCORA-Public/Publications/blob/master/04_OCORA%20Gamma%20Release/30_Program%20Documentation/OCORA-30-006-Gamma_High-Level-Methodology.pdf.

[3] FP2-R2DATO, 2024, D5.5 – Documentation of Freight specific user requirements for automation process. Publicly available online: https://www.ct5webapi.eu/api/documents/getfile?id=754b81c8-2835-435f-ae86-fbb3f3aa80da.

[4] OCORA Open CCS On-board Reference Architecture, 2020. Introduction, Gamma Release. Document ID: OCORA-30-001-Gamma. Version: 3.00. Available online: https://github.com/OCORA-Public/Publications/blob/master/04_OCORA%20Gamma%20Release/30_Program%20Documentation/OCORA-30-001-Gamma_Introduction.pdf

[5] OCORA Open CCS On-board Reference Architecture, 2025. Road Map, Release R6. Document ID: OCORA-BWS05-10. Version: 2.40. Available online: https://github.com/OCORA-Public/Publications/blob/master/00_OCORA%20Latest%20Publications/Latest%20Release/OCORA-BWS05-010_Road-Map.pdf

[6] OCORA Open CCS On-board Reference Architecture, 2025. Capella Modelling, Release R6. Available online: https://github.com/OCORA-Public/Publications/blob/master/12_OCORA%20Release%20R6/OCORA-TWS01-040_Capella-Modelling.pdf

[7] FP2-R2DATO, D38.2, Results of GoA1 remote controlled stabling and bringing a train to the station

[8] FP2-R2DATO, D38.3, Results of remotely monitored stabling and bringing a train to the station with remote monitoring

[9] FP2-R2DATO, D31.4, System analysis YTSM

[10] FP2-R2DATO, D31.5, Use case YTSM model report

[11] FP2-R2DATO, D6.5, ATO GoA3-4 Specifications and modelling

[12] FP2-R2DATO, D6.8, System Architecture Specification and Interface Specification for remote driving

[13] OCORA Open CCS On-board Reference Architecture, 2025. System Architecture, Release R6. https://github.com/OCORA-Public/Publications/blob/master/12_OCORA%20Release%20R6/OCORA-TWS01-030_System-Architecture.pdf