OCORA

Open CCS On-board Reference Architecture

Operational & System Analysis

Document ID: OCORA-TWS01-020

Version: 2.00

Date: 28.06.2022

Revision history

Version	Change Description	Initial	Date of change
1.00	Official version for OCORA Release R1	MT, JL, PV, TM, AL	03.12.2021
2.00	Official version for OCORA Release R2	MT, JL, PV, TM, AL, ML	23.06.2022

Table of contents

Table of figures

Table of tables

References

Reader's note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS04-010 – Problem Statements

[7] OCORA-TWS01-030 – System Architecture

[8] ISBN 978-1-78548-169-7 – Model-based System and Architecture Engineering with the Arcadia Method – Jean Luc Voirin – ISTE Press - 01/03/2018

[9] EEIG ERTMS Users Group, 21E158, Version 1.0, 06/09/21 - CCS Use Case Specification and Basic Requirements for the Intelligent Freight Train based on the DAC

1 Introduction

1.1 Purpose of the document

The purpose of this document is to provide a high-level view of all services that an OCORA based system provides to external actors, and to prepare for Europe's Rail Joint Undertakings System- & Innovation-Pillar. The document will evolve in subsequent releases. At a later stage, modelling of system capabilities is expected to be performed using a modelling tool such as Capella. To support the modelling activities, an operational analysis was initiated, and an initial set of system capabilities were derived from the elaborated operational activities.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

1.2 Applicability of the document

The document is currently considered informative. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of the OCORA release R2, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend to read the Introduction to OCORA [5], and the Problem Statements [6]. The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 Operational context

To support the operational analysis and to facilitate the identification of System Capabilities of the CCS-OB, OCORA identified the need for a high-level operational context of the different types of trains. The goal of this process is to help identifying the System Missions and high-level functional interactions of all actors of the CCS-OB.

2.1 Overview

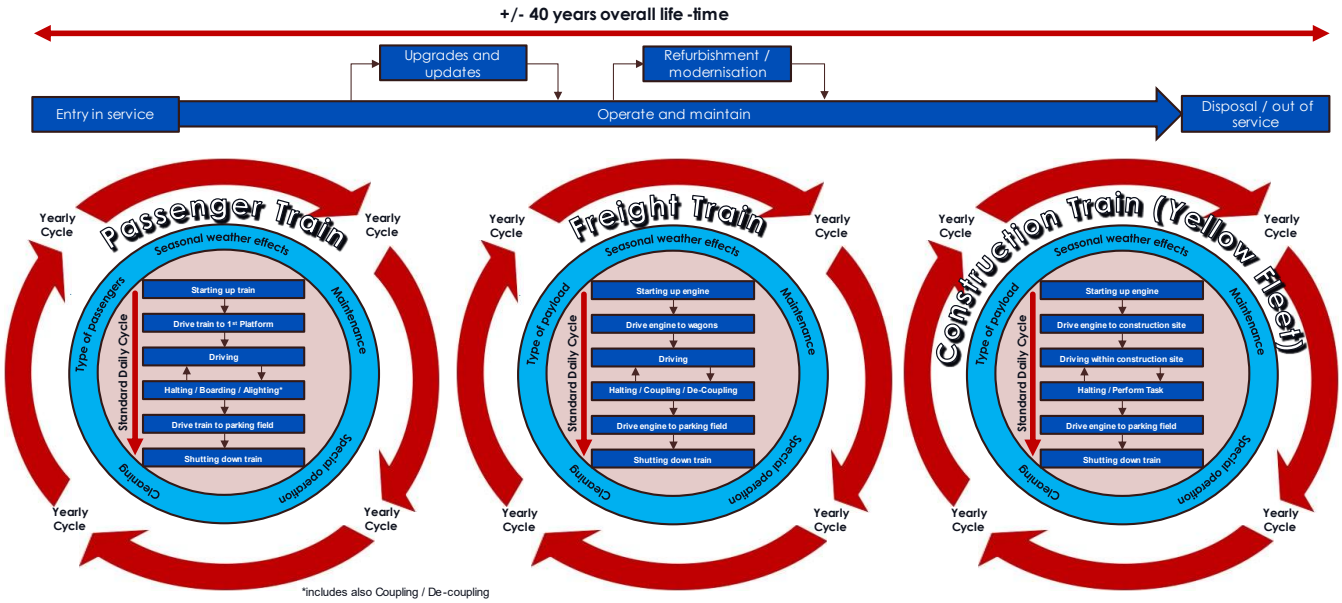


Figure 1 Operational concept overview

The high-level operational concept describes the production model of the operator: operational processes with a focus on rolling stock. The objective is to facilitate clear communication during the different project phases and provides context for expectations and user perspectives behind the formalised requirements. Within the V-model, the operational context is located at both upper ends of the V: it is an information source used when technical system requirements are written, but also the basis for validation activities. Considering the train within the context of operation, a framework of three different scales is central to this:

- A **day's cycle**. The daily cycle will cover the daily operational processes, from preparing the train for service until the end of service.
- A **yearly cycle.** The yearly cycles will zoom out further, assessing the weekly, monthly, and annual processes. This can cover both maintenance processes, atypical operational procedures, but also the influence of seasonal effects.
- The full **life cycle** from introduction up to and including the end of service and recycling. As the life cycle of the train will contain multiple life cycles of different IT systems, this perspective is the basis to prepare for regular updates and upgrades, ideally in sync with the longer maintenance cycles.

Combining the need different time frames, which will include a set of operational processes, serves as a first perspective to determine required capabilities of the CCS-OB, which is defined further in chapter 5.

3 Operational analysis

The operational analysis is conducted from the perspective of the whole train and the CCS-OB related to a standard daily cycle (refer to Figure 1). Activities covering longer term cycles like maintenance and the lifecycle are not considered at the current stage.

3.1 Overview

The following diagram shows the different states a train (respectively the CCS-OB) can be within a standard daily cycle. The operational states are described more precisely in section 3.2. The arrows between the different states define the possible transitions to reach another operational state (refer to section 3.2.7 for more details on the operational transitions). Each state encloses multiple operational activities which are elaborated and documented in the upcoming section 3.3.

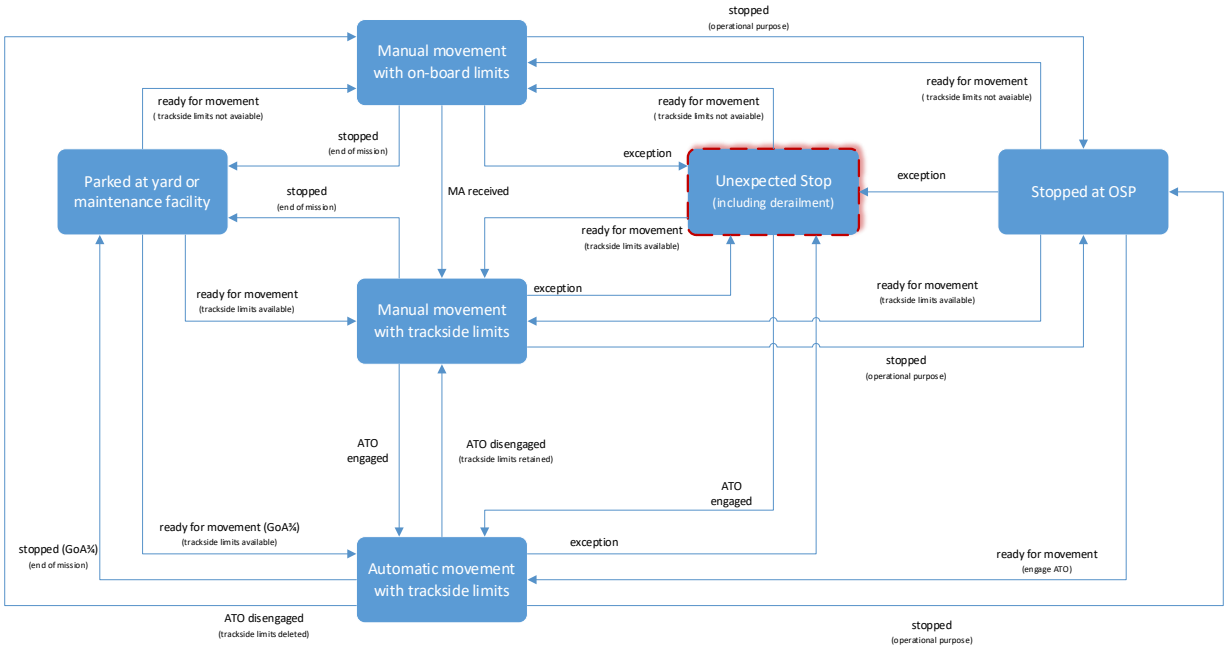


Figure 2 Operational states and transitions - overview

3.2 Operational states

3.2.1 Parked at yard or maintenance facility

The train is intentionally stopped in a yard or maintenance facility (parked at an appropriate location). The train either remains in this state for a longer period or in short it gets shut down.

3.2.2 Manual movement with on-board limits

The train is moving but has not yet received trackside information for a moving authority or this information has been deleted. The supervision of the train is limited, it is only based on some on-board parameters (e.g., ceiling speed).

3.2.3 Manual movement with trackside limits

The train is moving and has a moving authority based on information received from trackside. The position of the train is known.

3.2.4 Automatic movement with trackside limits

On the train, all operational and engagement conditions are fulfilled, and ATO-OB is engaged. The train is moving while ATO-OB automatically drives the train. A moving authority has been received from trackside.

3.2.5 Unexpected Stop

The train is stopped unexpectedly (not planned halt) due to different reasons like, emergency brake, failure on trackside, failure on the train, emergency on the train (e.g., fire), etc.

3.2.6 Stopped at Operational Stopping Point (OSP)

The train has stopped intentionally at the operational stopping point (OSP) according to the schedule.

3.2.7 Operational transitions

All operational transitions are related to the whole train from CCS on-board perspective.

Some operational transitions for ATO with GoA 3/4 are indicated for the sake of completeness to the best of one's knowledge. Nevertheless, many points remain open and are not clear and can be completed once a more detailed concept and additional information is available from the Shift2Rail group working on the ATO with GoA 3/4.

Origin state	Transition	Destination state	Description
Parked at yard or maintenance facility	Ready for movement (trackside limits not available)	Manual movement with on-board limits	The train starts moving but has not received trackside information for a moving authority or this information has been deleted. Train supervision is limited, it is only based on some on-board parameters (e.g., ceiling speed).
	Ready for movement (trackside limits available)	Manual movement with trackside limits	The train starts moving and has received a moving authority from trackside.
	Ready for movement (GoA¾) (trackside limits available)	Automatic movement with trackside limits	This is only valid for ATO with GoA 3/4. On the train all operational and engagement conditions are fulfilled and ATO-OB gets engaged. The train starts moving while ATO-OB automatically drives the train. A moving authority from trackside was received.
Manual movement with on-board limits	Stopped (end of mission)	Parked at yard or maintenance facility	The train intentionally stops in yard or in maintenance facility (parked in an appropriate location). The train either remains in this state for a longer period or in short it gets shut down.
	Moving Authority received	Manual movement with trackside limits	The train keeps moving but meanwhile it has a moving authority based on information received from trackside (e.g., first balise has been read).
	Exception	Unexpected Stop (including derailment)	The train unexpectedly stops moving (not planned halt) due to different reasons: emergency brake, failure on trackside, failure on the train, emergency on the train (e.g., fire).
	Stopped (operational purpose)	Stopped at OSP	The train intentionally stops at the next operational stopping point (OSP) according to schedule.
Manual movement with trackside limits	Stopped (end of mission)	Parked at yard or maintenance facility	The train intentionally stops in yard or in maintenance facility (parked in an appropriate location). The train either remains in this state for a longer period or in short it gets shut down.
	ATO engaged	Automatic movement with trackside limits	On the train all operational and engagement conditions are fulfilled and ATO-OB gets engaged. Now ATO-OB automatically drives the train.
	Exception	Unexpected Stop (including derailment)	The train unexpectedly stops moving (not planned halt) due to different reasons: emergency brake, failure on trackside, failure on the train, emergency on the train (e.g., fire).
	Stopped (operational purpose)	Stopped at OSP	The train intentionally stops at the next operational stopping point (OSP) according to schedule.

Origin state	Transition	Destination state	Description
Automatic movement with trackside limits	Stopped (GoA¾) (end of mission)	Parked at yard or maintenance facility	This is only valid for ATO with GoA 3/4. The train intentionally stops in yard or in maintenance facility (parked in an appropriate location). The train either remains in this state for a longer period or in short it gets shut down.
	ATO disengaged (trackside limits deleted)	Manual movement with on-board limits	On the train either any of the operational conditions but the ETCS related ones is no longer fulfilled or a condition for ATO disengaging occurs, ATO-OB no longer drives the train automatically. The train driver takes over and drives the train. Simultaneously the trackside information for a moving authority is deleted, therefore supervision is limited, it is only based on some on-board parameters (e.g., ceiling speed).
	ATO disengaged (trackside limits retained)	Manual movement with trackside limits	On the train either any of the operational conditions but the ETCS related ones is no longer fulfilled or a condition for ATO disengaging occurs, ATO-OB no longer drives the train automatically. The train driver takes over and drives the train.
	Exception	Unexpected Stop (including derailment)	The train unexpectedly stops moving (not planned halt).
	Stopped (operational purpose)	Stopped at OSP	The train intentionally stops at the next operational stopping point (OSP) according to schedule.
Unexpected Stop (including derailment)	Ready for movement (trackside limits not available)	Manual movement with on-board limits	The train starts moving but has not received trackside information for a moving authority or this information has been deleted. Train supervision is limited, it is only based on some on-board parameters (e.g., ceiling speed).
	Ready for movement (trackside limits available)	Manual movement with trackside limits	The train starts moving and has a moving authority based on information received from trackside. Train position is known.
	ATO engaged	Automatic movement with trackside limits	On the train all operational and engagement conditions are fulfilled and ATO-OB gets engaged. The train starts moving while ATO-OB automatically drives the train. The moving authority is based on information received from trackside. Train position is known.

Origin state	Transition	Destination state	Description
Stopped at OSP	Ready for movement (trackside limits not available)	Manual movement with on-board limits	The train starts moving but has not received trackside information for a moving authority or this information has been deleted. Train supervision is limited, it is only based on some on-board parameters (e.g., ceiling speed).
	Exception	Unexpected Stop (including derailment)	The train unexpectedly remains at halt (unplanned halt).
	Ready for movement (trackside limits available)	Manual movement with trackside limits	The train starts moving and has a moving authority based on information received from trackside. Train position is known.
	Ready for movement (engage ATO)	Automatic movement with trackside limits	On the train all operational and engagement conditions are fulfilled and ATO-OB gets engaged. The train starts moving while ATO-OB automatically drives the train. The moving authority is based on information received from trackside. Train position is known.

Table 1 Operational transitions

3.3 Operational activities

As a first step, the required operational activities to manage “a day in the life of a train”, are elaborated. The description (bullet points) lists the steps required, from a train drivers’ perspective, to fulfil the activity. This process provides the foundation for the next step - the identification of the system capabilities.

It must be noted that not all steps listed in the description field may involve the CCS-OB (e.g., activate compressor, activate brake system, etc.). They are listed for completeness and to support the understanding of the described operational activity. Furthermore, the list of operational activities is not complete and will evolve in the upcoming OCORA Releases.

		Initiating Actor(s)										Operational States						Description (bullet points)
ID	Operational Activity	Train Driver	Train Attendant	Passenger	Physical Train Unit	OCS-IM	OCS-RU	Eurobalise	Euroloop	Light Signal	Environment	Parked	Manual Movement OB limits	Manual Movement TS limits	Automatic Movement TS limits	Stopped at OSP	Unexpected Stop	
OpA001	Start-up train	x	-	-	-	-	-	-	-	-	-	x	-	-	-	x	x	**Leading** ▪ turn on control power (Battery) ▪ systems are initialising and performing health checks ▪ activate cabin ▪ check and confirm train composition (TCMS) ▪ raise pantograph or start diesel engine ▪ power train (main switch) - electric train only ▪ activate compressor ▪ activate brake system ▪ activate comfort system (e.g., air-conditioning, heating, etc.) ▪ activate passenger info system ▪ activate CAB radio (voice communication) ▪ check smoke detector system ▪ perform ETCS system test (EB test) ▪ perform dead man's switch test (Driver Safety Device (DSD)) ▪ turn lights on (inside and outside) ▪ test close & lock doors **Non-Leading** ▪ turn on control power (Battery) ▪ systems are initialising and performing health checks ▪ activate cabin ▪ check and confirm train composition (TCMS) ▪ raise pantograph or start diesel engine ▪ power train (main switch) - electric train only ▪ activate compressor ▪ activate comfort system (e.g., air-conditioning, heating, etc.) – if not controlled by leading engine ▪ activate passenger info system – if not controlled by leading engine ▪ activate CAB radio (voice communication) ▪ check smoke detector system – if not controlled by leading engine ▪ perform ETCS system test (EB test) ▪ perform dead man's switch test (Driver Safety Device (DSD)) ▪ turn lights on (inside and outside) – if not controlled by leading engine ▪ test close & lock doors – if not controlled by leading engine

ID	Operational Activity	Initiating Actor(s)										Operational States						Description (bullet points)
		Train Driver	Train Attendant	Passenger	Physical Train Unit	OCS-IM	OCS-RU	Eurobalise	Euroloop	Light Signal	Environment	Parked	Manual Movement OB limits	Manual Movement TS limits	Automatic Movement TS limits	Stopped at OSP	Unexpected Stop	
OpA002	Compose train	x	-	-	-	-	-	-	-	-	-	x	-	-	-	x	-	**Couple train engine to composition of coaches / wagons:** ▪ activate parking brake ▪ deregister CAB radio (voice) - if required ▪ main switch off ▪ lower pantograph stop diesel engine ▪ attach or detach coaches / wagons ▪ deactivate cabin ▪ walk to the other cabin ▪ activate cabin ▪ check and confirm train composition (TCMS) ▪ raise pantograph / start diesel engine ▪ power train (main switch) - electric train only ▪ activate compressor ▪ activate brake system ▪ activate comfort system (e.g., air-conditioning, heating, etc.) ▪ activate passenger info system ▪ deactivate parking brake ▪ check smoke detector system ▪ turn lights on inside/outside ▪ test close & lock doors **Attach additional coaches / wagons to train:** ▪ lower pantograph or stop diesel engine ▪ attach or detach coaches / wagons ▪ check and confirm train composition (TCMS) ▪ raise pantograph or start diesel engine ▪ power train (main switch) - electric train only ▪ activate compressor ▪ activate brake system ▪ activate comfort system (e.g., air-conditioning, heating, etc.) ▪ activate passenger info system ▪ check smoke detector system ▪ turn lights on inside/outside ▪ test close & lock doors
OpA003	Prepare train for mission	x	-	-	-	-	-	-	-	-	-	x	-	-	-	x	x	**Leading** ▪ enter/update CAB (voice) radio data ▪ enter/confirm passenger info data ▪ enter/confirm ETCS data (register with trackside) ▪ brake tests (incl. passenger emergency hand brake) **Non-Leading** ▪ enter/update CAB (voice) radio data ▪ enter/confirm passenger info data – if not controlled by leading engine ▪ select non leading mode (NL) on ETCS DMI
OpA004	Prepare train for departure	x	-	-	-	-	-	-	-	-	-	x	-	-	-	x	x	▪ approaching departure time ▪ authorization to move (MA from track signal or on DMI (cab signalling) or on-board limits (SR or RS) ▪ departure time reached (dwell time expired) ▪ authorisation from train attendant (if required) ▪ enforce closure & locking of doors (driver or attendant) ▪ all doors are locked
OpA005	Drive to operational stopping point	x	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	▪ accelerate and brake or coasting ▪ comply with trackside / on-board signals (e.g., stop at light signals, adapt speed, etc.) ▪ comply to journey profile (schedule) ▪ observe outside environment ▪ observe PTU (TCMS, manometers, emergency brake, smoke alarm, etc.) ▪ check train consistency (driving mirror) before entering longer tunnels (smoke, open doors, loose parts, etc.) ▪ repeatedly press dead man pedal ▪ release doors on correct side (on platform side) ▪ stop at platform (taking into account the train length)
OpA006	Communicate with passengers	x	-	-	-	x	x	-	-	-	-	-	x	x	x	x	x	▪ driver makes ad-hoc voice announcements ▪ driver plays pre-recorded announcements ▪ observe passenger information system (to ensure that correct announcements are made)
OpA007	Communicate with off-board staff	x	-	x	-	-	-	-	-	-	-	x	x	x	x	x	x	▪ passenger talks to off-board staff (emergency GoA3/4) ▪ driver talks to off-board staff (e.g., traffic controller, maintenance manager, etc.) ▪ driver interacts with selected track workers using sign language
OpA008	Communicate with on-board staff	x	x	x	-	-	-	-	-	-	-	x	x	x	x	x	x	▪ driver talks to train attendant ▪ train attendant talks to driver ▪ train attendants talk to each other ▪ passenger talks to train attendant (only in person communication)
OpA009	Passenger requests stop	-	-	x	-	-	-	-	-	-	-	-	x	x	x	x	-	▪ passenger presses stop-on-request button on-board ▪ driver is informed via indicator light ▪ driver observes if there are passengers on platform waiting for this train and decides to stop
OpA010	Passengers embark & disembark	-	x	x	-	-	-	-	-	-	-	-	-	-	-	x	-	▪ door open request ▪ driver observes if doors are opening ▪ passengers enter / leave train ▪ train attendant manages proper embarking/disembarking of passengers
OpA011	Load and unload cargo	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	▪ load master signals manually that loading/unloading has been completed

ID	Operational Activity	Initiating Actor(s)										Operational States						Description (bullet points)
		Train Driver	Train Attendant	Passenger	Physical Train Unit	OCS-IM	OCS-RU	Eurobalise	Euroloop	Light Signal	Environment	Parked	Manual Movement OB limits	Manual Movement TS limits	Automatic Movement TS limits	Stopped at OSP	Unexpected Stop	
OpA012	Joining trains	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	**Train at standstill**: ▪ prepare train for coupling (open hatch, if necessary, etc.) ▪ set couple mode (parking mode or parking mode and coupling mode) ▪ put cabin in standby mode (if this cabin will not be leading the coupled train) ▪ **If this cabin remains the leading cabin:** ▪ driver waits for completion of coupling ▪ deactivate parking mode ▪ check and confirm train composition (TCMS) ▪ enter/confirm passenger info data ▪ modify ETCS data ▪ brake tests (incl. passenger emergency hand brake) ▪ deactivate parking brake **Moving train**: prepare train for coupling (open hatch, if necessary, etc.) check if "Train to be attached" is in coupling mode couple change cabin
OpA013	Splitting train	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	**Train to be split**: ▪ activate parking mode ▪ select correct splitting point ▪ decouple ▪ retract coupling and close hatch if required **If this cabin remains a leading cabin:** ▪ deactivate parking mode ▪ enter/confirm passenger info data ▪ modify ETCS data ▪ deactivate parking brake ▪ if necessary, turn off lights in passenger coaches **If this cabin is no longer leading:** ▪ unregister CAB Radio ▪ deactivate cabin **Decoupled Train no longer in use:** ▪ remains in parking mode **Decoupled Train remains in use:** ▪ activate correct cabin ▪ deactivate parking mode ▪ activate brake system ▪ enter CAB (voice) radio data ▪ enter/confirm passenger info data ▪ enter/confirm ETCS data (register with trackside) ▪ brake tests (incl. passenger emergency hand brake) ▪ deactivate parking brake
OpA014	Change cabin	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	**In mode parking:** ▪ activate parking brake ▪ deregister CAB radio (voice) - if required ▪ activate parking mode ▪ deactivate cabin ▪ walk to the other cabin ▪ activate cabin ▪ deactivate parking mode ▪ activate brake system ▪ enter CAB (voice) radio data ▪ enter/confirm passenger info data ▪ enter/confirm ETCS data (register with trackside) ▪ brake tests (incl. passenger emergency hand brake) ▪ deactivate parking brake ▪ check smoke detector system ▪ test close & lock doors **Without parking mode:** ▪ activate parking brake ▪ deregister CAB radio (voice) - if required ▪ main switch off ▪ lower pantograph ▪ deactivate cabin ▪ walk to the other cabin ▪ activate cabin ▪ raise pantograph ▪ turn main switch on ▪ activate brake system ▪ enter CAB (voice) radio data ▪ enter/confirm passenger info data ▪ enter/confirm ETCS data (register with trackside) ▪ brake tests (incl. passenger emergency hand brake) ▪ deactivate parking brake ▪ check smoke detector system ▪ test close & lock doors

ID	Operational Activity	Initiating Actor(s)										Operational States						Description (bullet points)
		Train Driver	Train Attendant	Passenger	Physical Train Unit	OCS-IM	OCS-RU	Eurobalise	Euroloop	Light Signal	Environment	Parked	Manual Movement OB limits	Manual Movement TS limits	Automatic Movement TS limits	Stopped at OSP	Unexpected Stop	
OpA015	Change driver	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	**National value (N_NVDERUN) allows changing driver ID:** ▪ new driver enters cabin ▪ new driver enters new driver ID ▪ new driver checks ETCS data **National value (N_NVDERUN) prohibits changing driver ID:** ▪ current driver deactivates cabin ▪ new driver enters cabin ▪ new driver activates cabin ▪ execute system tests (initiate stationary brake test, check dead man switch, etc.) ▪ visual system check ▪ enter train data ▪ initiate voice radio communication ▪ register with trackside
OpA016	Drive to yard or maint. Facility (GoA 1/2) (shunting)	x	-	-	-	-	-	-	-	-	-	-	x	x	-	-	-	▪ select mode shunting ▪ wait for MA at the shunting signal ▪ accelerate and brake or coasting ▪ comply with track-side signals (e.g., shunting signals, adapt speed, etc.) ▪ observe outside environment (there might be obstacles on the way!) ▪ observe PTU (TCMS, manometers, emergency brake, smoke alarm, etc.) ▪ repeatedly press dead man pedal ▪ release doors (at maintenance facility) ▪ stop at yard / maint. facility (taking into account the train length)
OpA017	Drive to yard or maint. Facility (GoA3/4) (shunting)	-	-	-	-	x	-	-	-	-	-	-	-	-	x	-	-	▪ based on the mission profile mode ATO shunting is selected ▪ wait for MA from MT ▪ accelerate and brake or coasting ▪ perception system observes the track (obstacles), shunting signals and other signs, etc. ▪ react to track-side signals, signs, obstacles, etc. ▪ operator traffic control centre (TCC) observes PTU (TCMS, emergency brake, smoke alarm, etc.) ▪ release doors (at maintenance facility) according to mission profile ▪ stop at yard / maint. facility (taking into account the train length)
OpA018	End Mission	x	-	-	-	x	-	-	-	-	-	x	-	-	-	x	x	▪ deregister CAB Radio ▪ activate parking brake ▪ activate vehicle mode depending on local operational procedures e.g., parking mode, sleeping mode etc. ▪ deactivate cabin ▪ check full train to ensure nobody is left behind
OpA019	Shutdown train	x	-	-	x	-	-	-	-	-	-	x	-	-	-	x	x	▪ activate cabin (if not yet activated) ▪ deactivate parking mode or sleeping mode ▪ ensure that parking brakes are active ▪ Diesel engine: ▪ turn off diesel engines ▪ power off train ▪ Electric engine: ▪ turn off main switch ▪ lower pantograph ▪ power off train
OpA020	Manoeuvre at operational stopping point	x	-	-	x	-	-	-	-	-	-	-	x	-	-	-	-	▪ switch to manual movement with on-board limits (shunting mode) ▪ switch voice radio registration for shunting ▪ request and receive permission for manoeuvre ▪ communicate with shunter in case the sight onto the tracks is blocked ▪ accelerate and brake ▪ comply with track-side manoeuvre signals (e.g., stop at light signals) ▪ observe outside environment ▪ observe PTU ▪ stop at stopping point (taking into account the train length) ▪ deactivate shunting mode ▪ --> continue e.g., with OpA003 Prepare Train for Mission
OpA021	Manoeuvre in maintenance yard (non-centralized interlocking)	x	-	-	x	-	-	-	-	-	-	-	x	-	-	-	-	▪ switch to manual movement with on-board limits (shunting mode) ▪ switch voice radio registration for shunting ▪ set and verify correct position of switches ▪ communicate with shunter in case the sight onto the tracks is blocked ▪ accelerate and brake or coasting ▪ comply with track-side manoeuvre signals (e.g., stop at light signals) ▪ observe outside environment ▪ observe PTU ▪ stop at final position ▪ deactivate shunting mode

ID	Operational Activity	Train Driver	Train Attendant	Passenger	Physical Train Unit	OCS-IM	OCS-RU	Eurobalise	Euroloop	Light Signal	Environment	Parked	Manual Movement OB limits	Manual Movement TS limits	Automatic Movement TS limits	Stopped at OSP	Unexpected Stop	Description (bullet points)
		Initiating Actor(s)										Operational States						
OpA022	Manoeuvre in construction site (track barred to traffic)	x	-	-	x	-	-	-	-	-	-	-	x	-	-	-	-	This activity covers only the movement inside the construction area. Yellow fleet vehicles are usually not equipped with a CCS-OB. ▪ accelerate and brake ▪ observe outside environment ▪ observe PTU ▪ stop at final position **Vehicles with CCS-OB** ▪ switch to manual movement with on-board limits (shunting mode) ▪ accelerate and brake ▪ comply with on-board limits and track-side manoeuvre signals, if available ▪ observe outside environment ▪ observe PTU ▪ stop at final position ▪
OpA023	Evacuate passengers	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	x	**Complete train stopped at platform** ▪ Advise passengers to leave the train ▪ Unlock/open doors to platform **Partial train stopped at platform or on track** ▪ Communicate with traffic control centre ▪ Agree on evacuation concept ▪ Inform passengers ▪ Prepare evacuation ▪ Advise passengers according to evacuation concept ▪ Unlock/open required doors
OpA024	Drive reverse (reversing)	x	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	**ETCS L2 (only in tunnels)** ▪ Operation control centre initiates the reversing process ▪ CCS-OB receives “RV” mode ▪ Train driver set the direction control to backwards and confirms RV mode on CCS-OB (DMI or ETCS confirmation button) ▪ accelerate and brake ▪ comply with trackside limits (speed and distance) ▪ stop after RV end signal or trackside limit ▪ Communicate with OCC **ETCS L0/L1** ▪ Reversing does not exist - only in shunting mode
OpA025	Drive reverse (GoA3/4)	x	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	▪
OpA026	Drive non-leading	x	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	Train driver on non-leading engine ▪ Communicate by CAB voice with leading train driver ▪ Control traction according to instructions by leading train driver
OpA027	Drive non-leading (GoA3/4)	x	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	▪ TBD
OpA028	ATP isolation	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	▪ TBD
OpA029	Prepare train to be rescued	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	▪ TBD
OpA030	Join train to be rescue	x	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	▪ TBD
OpA031	Install software update	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	▪ TBD
OpA032	Install configuration update	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	▪ TBD
OpA033	Maintenance	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	x	▪ TBD
OpA034	Diagnostics	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	x	▪ TBD

Table 2 Operational Activities

3.4 Initiating Actors

For the description of the initiating refer to the OCORA System Architecture Document [7].

4 System analysis

Once the System under consideration is defined (scope and boundaries), the most natural way to compile the full set of System Capabilities is to follow a top-down approach and start by identifying Actors interacting with the System and Missions the System shall perform (see 4.2 System scope and actors and 4.3 Missions).

Knowing the Missions of a System is prerequisite to identify the System Capabilities necessary to accomplish those missions.

Again, Capabilities facilitate the identification of System Functions. Capabilities are described using one or multiple Functional Chain(s), Scenario(s) and Mode/State Diagram(s).

Functional Chains assist the RAMSS analysis, Scenarios describe the sequence of functions and their data exchanged. All resulting artefacts support the verification and validation process.

4.1 Definition of system capabilities

4.1.1 System capabilities in context of the Arcadia method

Ever-increasing expectations regarding functionality, safety, security, and performance of today's railway CCS systems, originating from different stakeholders, need to be managed and implemented in a structured and traceable way. The strength of any system is rooted in its architecture. The Arcadia method supports all required engineering activities that include analysing operational needs, structuring, and decomposing the system and considering constraints of existing standards and legislation as well as domain specific design objectives.

System Capabilities are a core element of the Arcadia methodology and defined [8] as follows:

"*A system capability is the system's expected ability to supply a service contributing to fulfilling one or more missions. A system capability represents a system usage context. It is characterized by a set of functional chains and scenarios that it references, and which more precisely describe the conditions for performing the system functions that contribute to it. A capability can also reference a function that contributes to it by itself.*

A capability can use one or more other capabilities that it will reference."

4.1.2 OCORA interpretation

For a better understanding, especially for people who are not familiar with the Arcadia method, capabilities may be considered services of the system provided to external actors. Capabilities are characterized, described, and illustrated using functions, scenarios, modes, and states.

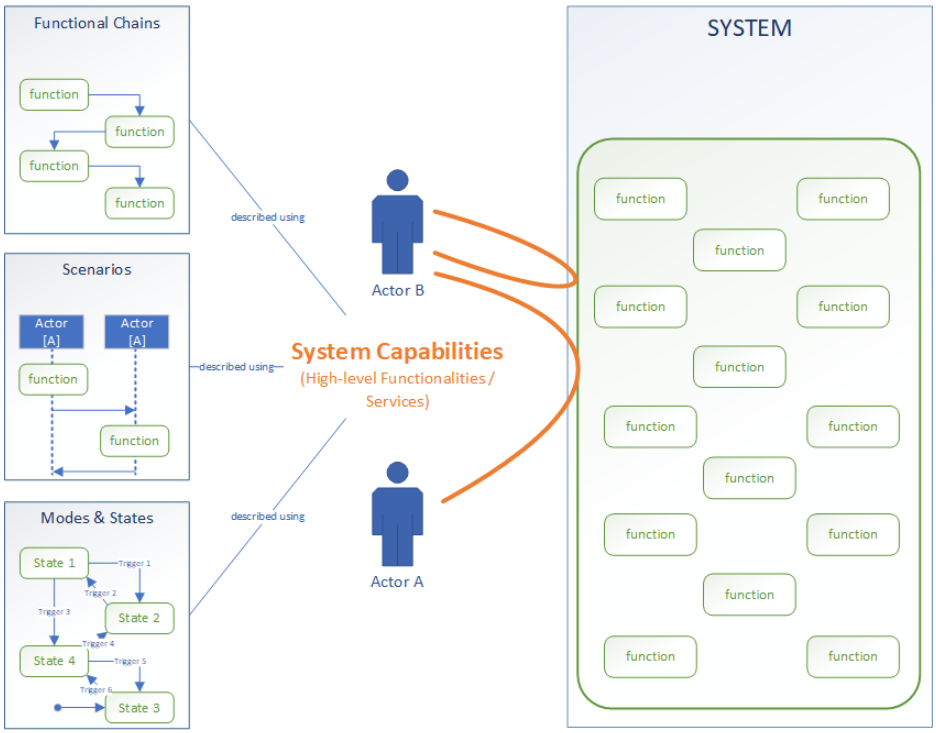


Figure 3 OCORA Perspective of System Capabilities

4.1.3 Arcadia approach

Arcadia stipulates a viewpoint-driven approach (as described in ISO/IEC 42010) and emphasizes a clear separation of need and solution.

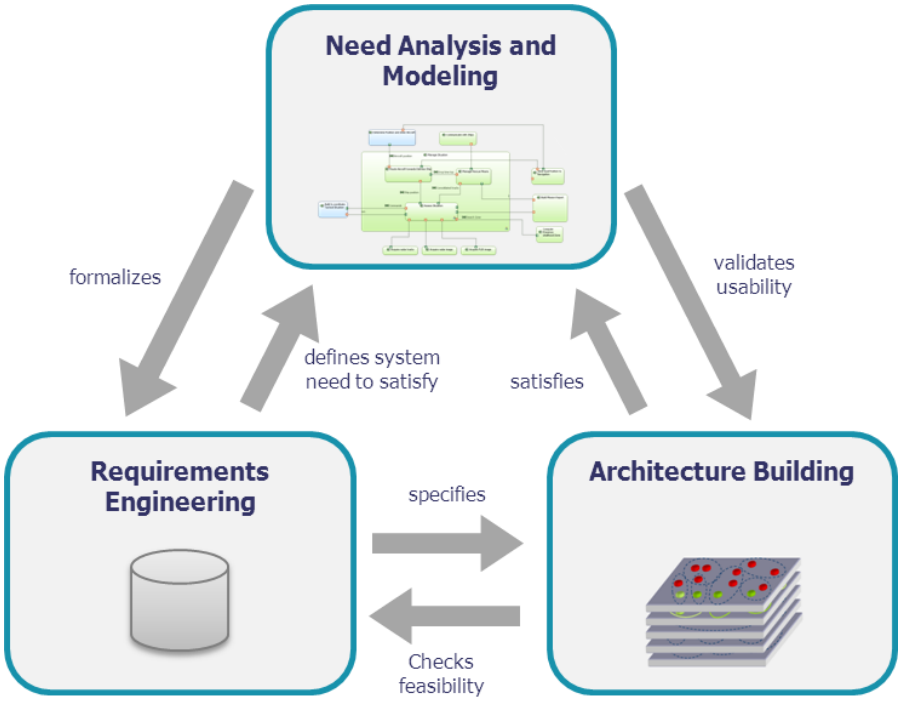


Figure 4 Viewpoint driven approach[1]

Arcadia promotes four[2] distinct perspectives:

- **Customer Operational Need Analysis** - definition of the Problem
  Focuses on analysing the customer needs and goals, expected missions and activities. It structures the need in terms of actors/users, their operational capabilities, and activities.

  Note: *Linx4Rail conducts an overall Operational Analysis. Synchronization shall happen at a later stage.*

- **System Need Analysis** - formalization of system requirements
  Focuses on the System itself, to define how it will satisfy the compiled operational need - zeroing in on functions and its related exchanges, non-functional constraints (e.g. safety, security, etc.) as well as role sharing between system and actors.

- **Logical Architecture (Notional Solution)** - definition of solution architecture
  Aims at building a coarse-grained component breakdown of the system. This involves taking important engineering decisions which are unlikely to be challenged at a later stage. The system is decomposed into logical components, functions are allocated to components. This building process is where the majority of the OCORA design objectives and design rules will be considered.

- **Physical Architecture** - definition of solution architecture
  Makes the logical architecture vision evolve according to implementation, technical and technological constraints, and choices.

[1] Source : https://www.eclipse.org/capella/arcadia.html
[2] Arcadia includes a fifth perspective regarding the Building Strategy. However, this perspective is currently considered to be out of scope of OCORA.

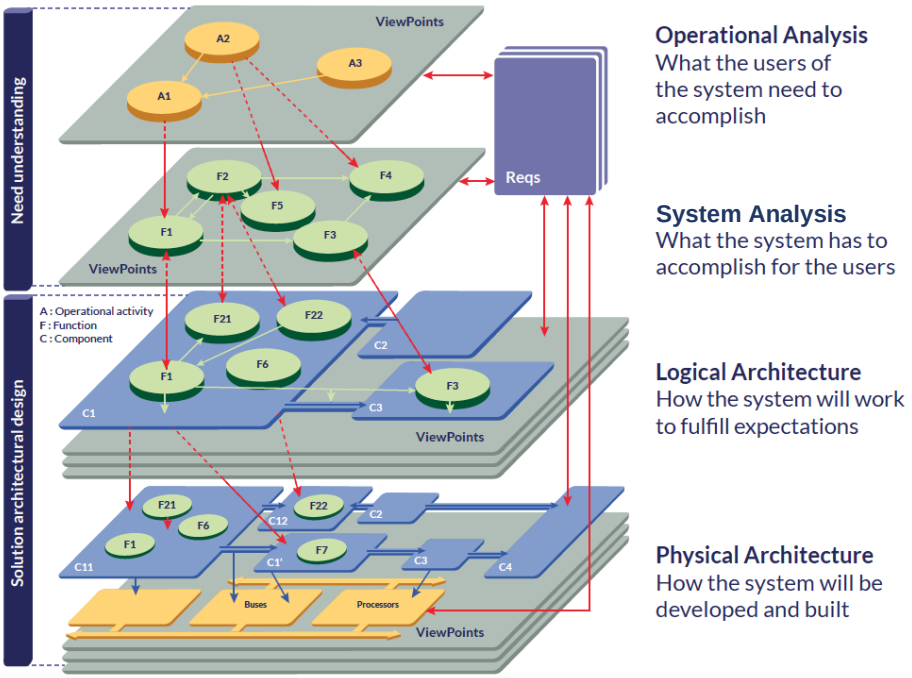


Figure 5 The four perspectives of Arcadia1

The Arcadia approach has been synchronized with the OCORA tailored V-model development process (see also Requirement - Management Guideline [9]).

Important Arcadia artefacts are:

Artefact	Description
System	The system is an ordered set of elements functioning as a whole, responding to customer and user demand and needs, and subject to engineering supported by Arcadia.
Actor	An actor is an entity that is external to the system (human or not), interacting with it, especially via its interfaces.
Mission	A mission is a high-level goal to which the system should contribute. To be fulfilled, a mission should use a number of system functions, regrouped within one or more system capabilities.
Capability	A system capability is the system's expected ability to supply a service contributing to fulfilling one or more missions.
Scenario	A function scenario is a time-ordered dynamic flow, on a temporal axis (conventionally vertical from top to bottom), of exchanges between different functions in the context of implementing a capability.
Functional Chain	A functional chain is an ordered set of references to functions and the functional exchanges that link them, describing one possible path among all the paths forming the dataflow.
Mode	A mode is a behaviour expected of the system, a component or also an actor or operational entity, in some chosen conditions.
State	A state is a behaviour undergone by the system, a component, an actor or an operational entity, in some conditions imposed by the environment.
Mode/state diagram	A mode(s) machine (or respectively, state(s) machine) is a set of modes (or, respectively, states) linked to one another by transitions. Modes and states cannot cohabit in the same machine.

Table 3 Arcadia Artefacts explained

[1] Source : https://www.eclipse.org/capella/arcadia.html

The following figure shows the relationship between Capabilities and other Arcadia modelling artefacts:

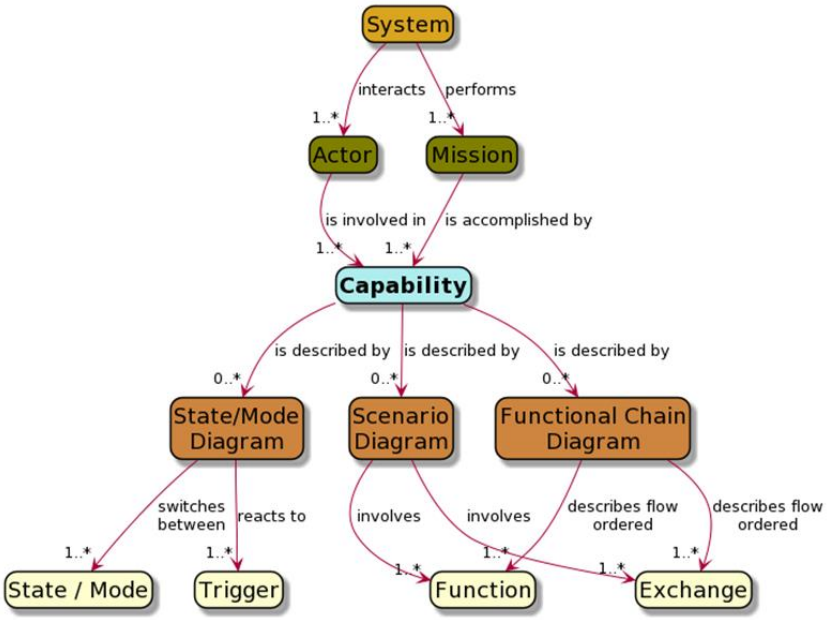


Figure 6 Artefacts of the System Analysis perspective

4.2 System scope and actors

As a first step for defining the Missions and System Capabilities, the scope and corresponding actors are identified.

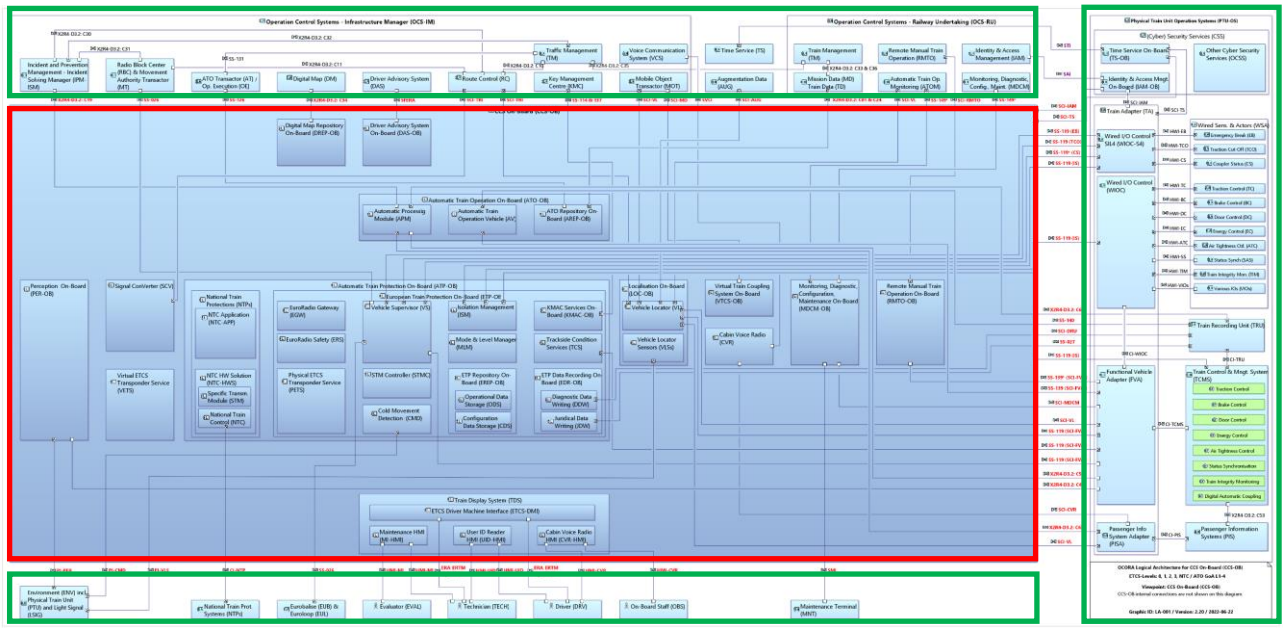


Figure 7 System under consideration (red) and Actors (green)

Note: The System under Consideration (SuC) is CCS On-Board only e.g., excluding the Train Adaptor. Nevertheless, OCORA aims to standardize the interface to the Physical Train Unit by leveraging existing standards and proposing improvements where necessary. Legacy trains require a Train Adaptor that translates legacy interfaces and behaviour; future trains, however, will implement the standardized interfaces natively, and will no longer need a Train Adaptor.

4.3 Missions

OCORA has identified the following missions the CCS-OB has to fulfil.

Ref.	Mission	ERTMS Level	GoA [1]	Comments
Mission 1	Control safe train movement.	0 1 2 3 NTC	1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4	This mission is related to Automatic Train Protection (ATP). Supervise safe train movement according to train configuration, track configuration, speed profile, permitted travel distance, assigned mode, current speed, and current position. This mission includes the triggering of EB and TCO.
Mission 2	Optimise (energy, capacity, comfort) train movement (command train or signal to driver).	0[2] 1 2 3 NTC	1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4	This mission is related to Automatic Train Operation (ATO). Command train movement and release door opening according to train configuration, segment profile (topology), journey profile (schedule), mission profile, perceived environment information (e.g., clearance profile), speed profile, permitted travel distance, assigned GoA level, current speed, and current position (GoA2-4). Signal information to the driver about actual speed and the optimal speed profile (GoA1 only).
Mission 3	Signal information to ensure safe and appropriate driving.	0 1 2 3 NTC	1, 2 1, 2 1, 2 1, 2 1, 2	This mission is related to ATP Cabin Signalling. Signal the mode of the ATP System and provide information to the driver about actual speed, maximum speed profile and the position within the permitted travel distance.
Mission 4	Provide voice communication means	0 1 2 3 NTC	1, 2 1, 2 1, 2 1, 2 1, 2	This mission is related to Cabin Voice. ▪ Voice communication between the Operations Control Systems personnel of the Infrastructure Manager and the Train Driver (TRDR). ▪ Voice communication between driver and train attendant ▪ Voice communication between driver and passenger
Mission 5	Provide information to the train system	0 1 2 3 NTC	1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4 1, 2, 3, 4	Provide communication means between trackside and the train systems ▪ Data communication between the Operations Control Systems of the Infrastructure Manager (OCS-IM) and the Physical Train Unit (PTU. ▪ Data communication between the Trackside Equipment (TSE) and the Physical Train Unit (PTU). Provide information computed by the CCS (odometry, speed) Provide information entered by the driver (e.g., ID, Train running number)

Remark: The maintenance of the system under consideration (CCS-OB) is not considered to be a mission of the system. For Level 0, Level 1 and Level NTC a system (e.g., perception, Euro-Loop, TVM, LZB) capable to provide track side signal information is needed to run in GoA3 and GoA4.

[1] The applicability of GoA with the ERTMS level needs to be verified by the ATO team (OCORA internal GitHub issue #259)
[2] The applicability of ERTMS Level 0 for this mission needs to be verified and will be updated in an upcoming OCORA Release

4.4 CCS-OB modes

By refining the operational states of the whole train (refer to 3.2) and setting the focus closer onto the CCS-OB the following CCS-OB operational modes have been identified.

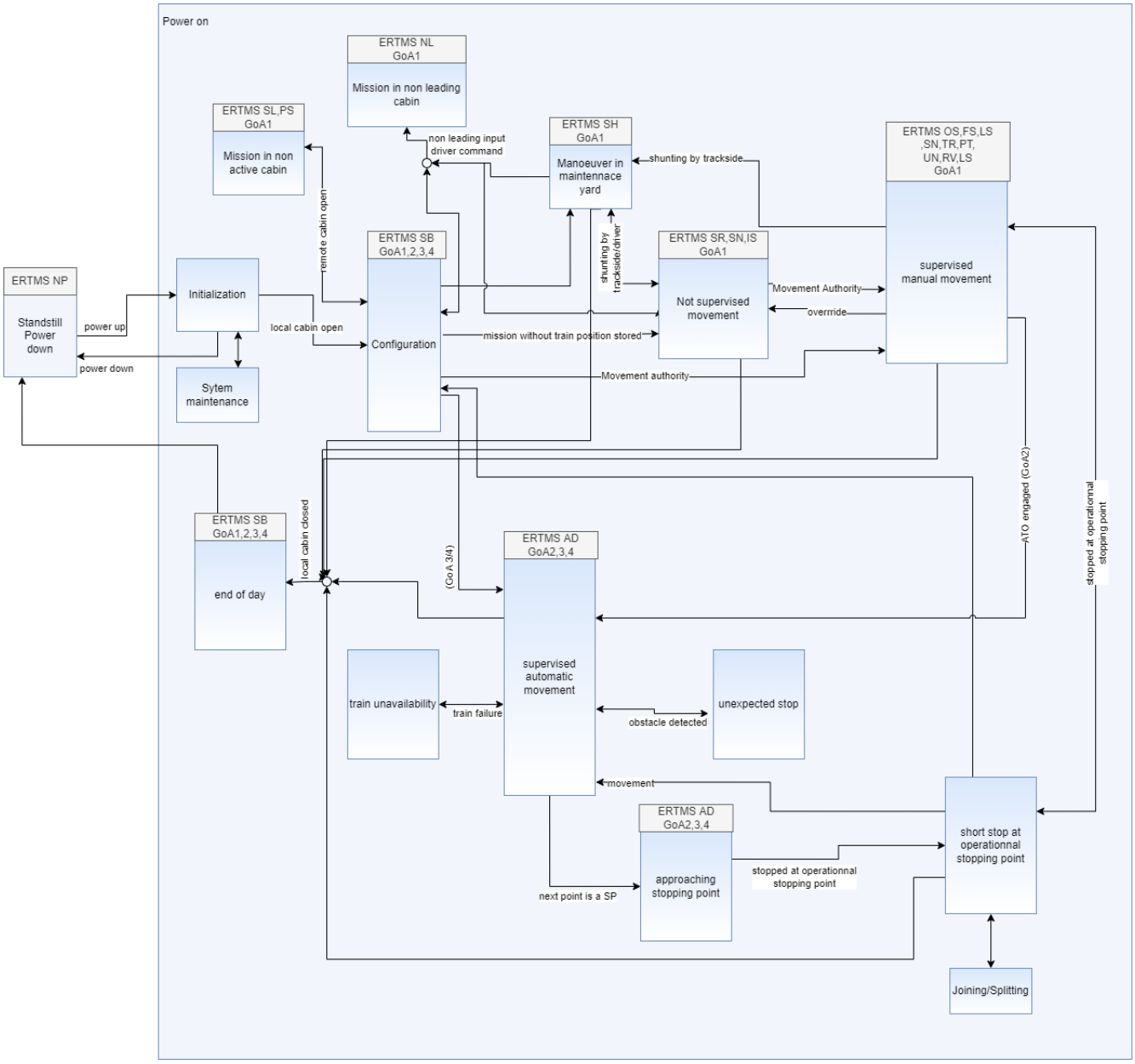


Figure 8 CCS-OB modes

The following table describes the different CCS-OB modes and an initial mapping to the ERTMS modes and operational states elaborated in the operational analysis (3.2).

CCS-OB mode	ERTMS modes	Description	Related operational state
System maintenance	-	A technician connects his maintenance terminal to the CCS in order to check internal state of the system. It performs update of software and configuration. It calibrates sensor. The system maintenance online can be performed on the train or in a test bench. In that case, each subsystem can be tested separately. CCS can have a specific technical mode in order to enable specific maintenance function.	▪ Parked at yard or maintenance facility

CCS-OB mode	ERTMS modes	Description	Related operational state
Standstill power down	NP	The system is not powered and does not provide any functionality	▪ Parked at yard or maintenance facility ▪ Unexpected Stop ▪ Stopped at OSP
Initialization	-	CCS performs its self-test. Subsystems connect and synchronize to each other. CCS evaluates, if new parameter or new software are available and performs the update. Stored configuration parameters are loaded and broadcasted to all consumers.	▪ Parked at yard or maintenance facility
Configuration	SB	CCS waits for configuration information from external system. Driver enters its ID and the train running number, enters the train data and configure the system (radio parameter e.g.). The train also transmits information (driver ID, train running number). CCS tries to connect with trackside systems. Driver selects the mode of the mission.	▪ Parked at yard or maintenance facility
Not supervised movement	SR, SN, IS	CCS doesn't know the position of the train. No movement authority is supervised. The train is running under the driver's responsibility.	▪ Manual movement with on-board limits
Supervised manual movement	OS, FS, LS, SN, TR, PT, UN, RV	CCS supervised static speed restriction and end of movement based on stored information which are frequently refreshed by RBC or infill equipment. It is located by referring to the group of beacons it crosses. CCS displays driving information (signalling and planning) to the driver and requests acknowledgement. Driver interacts with CCS to acknowledge or activates function. CCS manages transition to not supervised movement and to automatic movement (GoA2). CCS requests activation of train functions (e.g., lower/raise pantograph)	▪ Manual movement with trackside limits
Supervised automatic movement	AD	CCS performs same action as in supervised manual movement. In addition, CCS receives mission characteristic, computes an optimal driving profile and requests traction/brake to the train. The driving profile is based on timing points. In GoA4, the scope CCS supervises the environment through perception system and the set of train function managed is larger.	▪ Automatic movement with trackside limits
Approaching a stopping point	AD	CCS switches from timing point targets to location-based target. It aims to stop precisely to operational stopping point (station e.g.).	▪ Automatic movement with trackside limits
End of day	SB	CCS set the train for the "end of day" configuration.	▪ Parked at yard or maintenance facility
Short stop at operational stopping point	-	CCS manages the doors and control the train immobilization. It manages train change of configuration (cabin status, direction controller).	▪ Stopped at OSP
Joining/splitting	-	CCS supervises the train joining and command the traction/brake (precise speed and positioning). CCS configures the train (open coupler flap). And update its internal data	▪ Stopped at OSP
Train unavailability	-	CCS detects failure and takes immediate action ensuring safety. CCS command train function as a remediation of the situation (isolation for e.g.).	▪ Unexpected Stop
Unexpected stop	-	CCS detects trackside (obstacle for e.g.) disturbance and acts accordingly (stop for e.g.)	▪ Unexpected Stop
Manoeuvre in maintenance yard	SH	CCS supervises train movement according to speed restriction and list of allowed encountered balises. The movement occurs in maintenance yard/depot or work area.	▪ Manual movement with on-board limits
Mission in non-leading cabin	NL	CCS displays driving information (speed, track condition) to the driver and performs request to the train to enable specific functions (panto, main switch, etc.).	▪ Manual movement with trackside limits
Mission in rear cabin	SL/PS	CCS manages information and configuration in order to keep the capacity to ensure supervised movement (train position, RBC handover)	▪ Manual movement with trackside limits

Table 4 CCS-OB modes

4.5 System capabilities

For each operational activity identified during the operational analysis, the system capabilities were elaborated by walking through all the steps (bullet points) noted in the operational activity table and then by determining, if the CCS-OB is involved and what capability it needs to provide for this step.

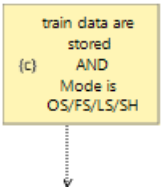
The following table contains an initial set of system capabilities and the mapping with the operational activity.

#	System Capability	OpA001 Start-up train	OpA002 Compose train	OpA003 Prepare train for mission	OpA004 Prepare train for departure	OpA005 Drive to operational stopping point	OpA006 Communicate with passengers	OpA007 Communicate with off-board staff	OpA008 Communicate with on-board staff	OpA009 Passenger requests stop	OpA010 Let passengers embark & disembark	OpA011 Load and unload cargo	OpA012 Joining trains	OpA013 Splitting train	OpA014 Change cabin	OpA015 Change driver	OpA016 Drive to p/m Facility (GoA1/2)	OpA017 Drive to p/m Facility (GoA3/4)	OpA018 End of Mission	OpA019 Shutdown train	OpA020 Manoeuvre at operational stopping	OpA021 Manoeuvre in maintenance yard	OpA022 Manoeuvre in construction site	OpA023 Evacuate passengers	OpA024 Drive reverse	OpA025 Drive reverse (GoA3/4)	OpA026 Drive non-leading	OpA027 Drive non-leading (GoA3/4)	OpA028 ATP isolation	OpA029 Prepare train to be rescued	OpA030 Join train to be rescued	OpA031 Install software update	OpA032 Install configuration update	OpA033 Maintenance	OpA034 Diagnostics
SysC01	Allow local system configuration	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-
SysC02	Allow remote system configuration	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-
SysC03	Manage train door operation	x	x	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC04	Allow mode selection by trackside	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	x	x	-	-	-	-	x	-	-	-	-	-	-	-
SysC05	Drive train between two operational timing points (ATO over ETCS)	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC06	Manage operational stopping points	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC07	Perform transition between GoA levels	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC08	Manage track conditions	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	-	-	-	-	-	-	-
SysC09	Command train function (GoA3/4)	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-
SysC10	Perform train coupling	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC11	Deactivate systems	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC12	Manage unattended stop	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC13	Provide driving advisory	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC14	Provide allowed speed and distance information	-	-	-	x	x	-	-	-	-	-	-	-	-	-	-	x	-	-	-	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-
SysC15	Allow RBC to command emergency stops	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	x	-	x	x	x	-	-	-	-	-	-	-	-

#	System Capability	OpA001 Start-up train	OpA002 Compose train	OpA003 Prepare train for mission	OpA004 Prepare train for departure	OpA005 Drive to operational stopping point	OpA006 Communicate with passengers	OpA007 Communicate with off-board staff	OpA008 Communicate with on-board staff	OpA009 Passenger requests stop	OpA010 Let passengers embark & disembark	OpA011 Load and unload cargo	OpA012 Joining trains	OpA013 Splitting train	OpA014 Change cabin	OpA015 Change driver	OpA016 Drive to p/m Facility (GoA1/2)	OpA017 Drive to p/m Facility (GoA3/4)	OpA018 End of Mission	OpA019 Shutdown train	OpA020 Manoeuvre at operational stopping	OpA021 Manoeuvre in maintenance yard	OpA022 Manoeuvre in construction site	OpA023 Evacuate passengers	OpA024 Drive reverse	OpA025 Drive reverse (GoA3/4)	OpA026 Drive non-leading	OpA027 Drive non-leading (GoA3/4)	OpA028 ATP isolation	OpA029 Prepare train to be rescued	OpA030 Join train to be rescued	OpA031 Install software update	OpA032 Install configuration update	OpA033 Maintenance	OpA034 Diagnostics
SysC16	Provide status information (ATP -ATO status)	x	x	x	-	x	-	-	-	-	-	x	x	x	x	x	x	x	-	-	x	x	x	x	x	x	-	x	-	-	x	x	-	-	-	-
SysC17	Supervise train speed and distance	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	x	-	x	x	-	-	-	-	-	-	-	-	-
SysC18	Manage train integrity	-	-	x	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	x	-	x	x	-	-	-	-	-	-	-	-	-
SysC19	Protect against undesirable train movement	x	x	x	x	-	-	-	-	-	-	-	-	-	x	-	-	-	x	x	-	-	-	-	x	-	-	-	-	-	x	x	-	-	-	-
SysC20	Allow driver to initiate supervised shunting	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC21	Acquire mission specific parameter	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC22	Manage trackside disturbance	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	x	-	x	x	x	-	-	-	-	-	-	-	-	-
SysC23	Manage Passengers incident	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC24	Manage rolling stock failures	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	x	-	x	x	x	-	-	x	x	-	-	x	x	
SysC25	Provide juridical record	x	x	x	x	x	-	-	-	-	-	-	x	x	x	x	x	x	x	x	x	x	x	-	x	x	x	x	x	x	x	-	-	x	x	
SysC26	Ensure communication between driver and train attendant/passenger	-	-	-	-	-	x	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC27	Ensure passenger communication without staff on board	-	-	-	-	-	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-
SysC28	Inform about on-board failure	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC29	Inform about infrastructure failure	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC30	Share information with the PTU	x	x	x	x	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	x	x	x	-	-	-	-	-	-	-
SysC31	Share information with the RBC	x	x	x	-	x	-	-	-	-	-	-	-	x	x	x	x	x	x	-	x	x	x	-	x	x	x	-	-	-	-	-	-	-	-	-
SysC32	Allow to set balises to be ignored by CCS-OB	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	x	-	x	x	x	-	-	-	-	-	-	-	-	-
SysC33	Allow to perform maintenance task and system test	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC34	Manage dwell time (GoA2)	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC35	Ensure communication between driver and off-board staff	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
SysC36	Manage stop request from passenger	-	-	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Appendix A System Capabilities template

OCORA is planning to use the following template for identifying and describing, on a high level, the capabilities. Mandatory fields are marked with an (M) and attributes also foreseen in Capella are identified with an *.

Name*	(M)	Name of the Capability. The following pattern is required: SysC<*capability number*>: <*capability name*> <*capability number*> is a unique integer number. <*capability name*> begin with an action verb which has optionally an object.
Operational Context*		Operational need of the Capability from a stakeholder perspective. Can be expressed as a user story. For example: As <*stakeholder name*>, the system helps me to <*system capability*> in order to carry out <*mission*>. As <*stakeholder name*>, I want to <*receive benefit*> from the system, when <*precondition*>, so that I can <*mission*>.
Summary*		Detailed description of the Capability. Can be expressed as a user story. For example: As <*actor name*>, the system helps me to <*system capability*> in order to carry out <*mission*>. As <*actor name*>, I want to <*receive benefit*> from the system, when <*precondition*>, so that I can <*mission*>.
Mission	(M)	Mission(s) related to the Capability as defined in the chapter 4.3.
Involved actors*		It includes human, non-human actors, and the system itself. Actors are defined in the chapter 4.2. Minimum one actor is referenced.
ERTMS Level*	(M)	Applicable ERTMS Level: 0, 1, 2, 3 or NTC.
ERTMS Mode*	(M)	Applicable ERTMS Mode (e.g., NP, OS, LS, FS, etc.)
GoA*	(M)	Applicable level of automation: 1, 2, 3 or 4.
Pre-condition*		Conditions necessary for the Capability to be performed. Must be selected from the list of Constraints and/or States in the System Analysis. It can be expressed as: a constraint that evaluates to TRUE or, an entering state of the system. A constraint is a Capella element which allow to formalize list of conditions carried by an element (function, a functional exchange). E.g.: 
Condition during execution		
Post-Condition*		Conditions verified after the Capability has been performed. Must be selected from the list of Constraints and/or States in the System Analysis. It can be expressed as: a constraint that evaluates to TRUE or, an existing state of the system. It is a measurable or observable result delivered by the system to an actor.
Non-Functional Requirement		Non-functional requirement applicable to the capability.
Functional Chain*	(M)	Functional chain(s) describing the Capability. Functional chain is an ordered sequence of functions linked with directional functional exchange or sequence link. Minimum one functional chain referenced. Generally, one functional chain by system mode where the capability is operating.

Scenario	(M)	Scenario describes a time sequence of exchange between actors (exchange scenario) or functions (functional scenario).
CCS-OB mode	(M)	Reference to an operational phase, as identified in chapter 4.4.
Type of train*	(M)	Type of train to which this capability is applicable (e.g., Passenger, Freight, Construction, All)
Remark		

Appendix B System Capabilities examples

This section provides some initial examples of prepared system capability descriptions, which will be used for the modelling tasks in Capella.

B1 SysC03 – Manage train door operation

Name*	(M)	**SysC03 - Manage train door operation**
Operational Context*		As a driver, I want to see if all doors are locked to ensure a safe departure and driving. As a driver, I want to see if passengers may open the doors to ensure an efficient passenger exchange. As a driver, I want to be advised when and on which side of the train to release the doors to allow passengers to open the doors. As a driver, I want to be advised when to close & lock the doors for an on-time safe departure. As an IM, I want the doors to be released or closed & locked automatically to ensure on-time departure. As a driver, I want to be informed if the doors are automatically being closed to understand what the system is doing.
Summary*		As a driver, I want the system to display the state of the doors (open, closed) As a driver I want the system to advise me about expected manual actions related to the doors. As a driver, I want the system to automatically operate the doors As a driver I want the system to display all automatically performed actions related to the doors (doors are being closed by ATO).
Mission	(M)	▪ Mission 2: Optimise (energy, capacity, comfort) train movement (command train or signal to driver).
Involved actors*		▪ Driver ▪ ATO Transactor ▪ Physical train unit ▪ Technician
ERTMS Level*	(M)	1,2,3
ERTMS Mode*		FS, AD
GoA*	(M)	1, 2
Pre-condition*		▪ The physical train unit is capable to provide the current state of the doors to the CCS-OB. AND ▪ CCS-OB is equipped with ATO AND ▪ ATP-OB is in FS or AD Mode
Condition during execution		
Post-Condition*		▪ Door information is displayed ▪ Door operation is performed

Non-Functional Requirement		ERA 15560 (CR1238)
Functional Chain*	(M)	▪ ATO transactor provides journey profile to CCS-OB ▪ PTU provides the states of the doors ▪ CCS-OB (ATO) determines the required door states ▪ CCS-OB (ATO) computes the door information to be displayed ▪ CCS-OB displays the door information to the driver. ▪ CCS-OB requests door operation ▪ PTU commands door operation
Scenario	(M)	▪ Train stops at station and the driver commands manually the door control ▪ Train stops at station and the ATO commands automatically the door control
Operational Phase	(M)	• Supervised manual movement • Supervised automatic movement • Short stop at operational stopping points • Approaching stopping point
Type of train*		Passenger
Remark		This capability is only active with ATO as it requires door information in Journey Profile from ATO transactor. Door information is displayed also in mode FS, when the ATO is not engaged when the train stops at station.

B2 SysC05 - Drive train between two operational timing points

Name*	(M)	**SysC05 - Drive train between two operational timing points (ATO over ETCS)**
Operational Need*		As an IM I want the train to drive automatically between two operational timing points whilst complying with the operational timetable to save energy and to improve passenger comfort.
Summary*		As a train, I want the system to provide me with traction/brake commands in order to move according to the operational timetable.
Mission	(M)	▪ Mission 2: Optimise (energy, capacity, comfort) train movement (command train or signal to driver).
Involved actors*		▪ PTU ▪ ATO transactor ▪ MT
ERTMS Level*	(M)	1,2,3, NTC
ERTMS Mode*		ERTMS mode AD
GoA*	(M)	2,3,4
Pre-condition*		▪ Journey profile and at least first segment profile have been received from ATO AND ▪ Movement authority has been received from MT AND ▪ ATO-OB is engaged
Condition during execution		
Post-Condition*		▪ The train reached last passing point before a stopping point
Non-Functional Requirement		Timing point accuracy - subset 125
Functional Chain*	(M)	▪ CSS-OB periodically checks with AT for updated journey profile ▪ CCS-OB (VL) determines train position

		▪ CCS-OB (ATO-OB) calculates the most efficient speed profile ▪ CCS-OB (ATO-OB) sends traction and brake commands to the train. ▪ PTU provides information about train status (brake/traction) ▪ CCS-OB requests next segment profile Note: CCS(ATO-OB) ensures the required stopping accuracy (max overshoot, max undershoot)
Scenario	(M)	▪ nominal following JP setpoint ▪ nominal following ERTMS curves ▪ profile update during mission
Operational Phase	(M)	▪ Supervised automatic movement
Type of train*		All

B3 SysC08 - Manage track conditions

Name*	(M)	**SysC08 - Manage track conditions**
Operational Need*		As an IM I want to be able to communicate track conditions to running trains to trigger (manually/automatically) the necessary actions when approaching or reaching a certain point. As a driver I want to see an indication about upcoming track conditions that require an action or attention. As a driver I want to be informed when I need to consider a track condition or execute an action based on a track condition. As a driver I want to be informed about track conditions that trigger an automatic action to be able to supervise automatic actions.
Summary*		As a Train, I want the system to help me perform actions based on received track condition As a driver, I want the system to help me perform and supervise actions based on received track conditions. ***Note***: Track condition = p68, p69 and “national” track conditions received from an NTP
Mission	(M)	▪ Mission 3: Signal information to ensure safe and appropriate driving ▪ Mission 5: Provide information to the train system
Involved actors*		▪ PTU ▪ CCS trackside: Movement authority Transactor (MT) (RCA trackside) / RBC (“old/legacy” trackside), Eurobalise (EUB), Euroloop (EUL), Radio Infill, National Train Protection Systems (NTPs) ▪ Driver
ERTMS Level*	(M)	1, 2, 3, NTC
ERTMS Mode*		▪ FS, LS, OS, NL, TR, PT (for track condition sent by the ETCS trackside) ▪ SN (for national track condition sent by an NTP) ▪ SR, SH, PS, UN, SB (big metal masses only)
GoA*	(M)	1, 2, 3, 4
Pre-condition*		▪ CCS-OB is configured to handle each track condition (manual or automatic)
Condition during execution		
Post-Condition*		▪ Track condition is handled.
Non-Functional Requirement		
Functional Chain*	(M)	▪ CCS trackside (MT / RBC, EUB, EUL, Radio infill, NTPs) provides track conditions ▪ CCS-OB determines the action(s) to be performed based on the received track conditions and the train location.

		▪ CCS-OB displays track conditions information to the driver ▪ CCS-OB sends track conditions commands to the PTU ▪ PTU performs the actions based on the track conditions ▪ Driver supervises action(s) executed based on the track conditions ▪ Driver performs action(s) based on track conditions
Scenario	(M)	▪ Track conditions received from ETCS trackside. ▪ Track conditions received from NTC. ▪ Reception of a new track conditions list when a previously one is stored on-board but not yet executed. ▪ Reception of a new track conditions list when a previously one is stored on-board and being executed. ▪ Shortening track descriptions when the train is inside a track condition ▪ Reset to initial state ▪ Train receives track conditions when there are already 3 icons displayed on the DMI
Operational Phase	(M)	▪ Mission in NL cab. ▪ Not supervised movement (big metal masses TC) ▪ Shunting in maintenance yard (big metal masses TC) ▪ Supervised manual movement ▪ Supervised automatic movement ▪ Approaching stopping point ▪ Short stop at operational stopping point
Type of train*		All