Rail to Digital automated up to autonomous train operation

D5.4 – Documentation of use cases for Remote Driving

Due date of deliverable: 30/11/2023

Actual submission date: 01/12/2023

Leader/Responsible of this Deliverable: Francesco Inzirillo MERMEC

Reviewed: Y

Document status		
Revision	Date	Description
01	25/10/2023	First issue.
02	03/11/2023	Issued in the context of internal review FP2-T5_4-C-MER-011-01 to initiate TMT review.
03	07/11/2023	Review report FP2-T5_4-C-MER-011-01 now issued. TMT review resumed.
04	01/12/2023	Review after TMT comments FP2-TMTRev-R-GTD-072-02, including Alstom partner feedback FP2-T5_4-T-MER-027-01.
05	31/01/2024	Introduction of the accepted comments receive from external source FP5 and FP6 experts.
06	16/02/2024	Introduction of accepted additional comments from FP5

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

Start date: 01/03/2023 Duration: 9 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
Inzirillo Francesco	MERMEC	Task 5.4 Lead, Specification
Pierre Le Maguet	GTDS	Specification, Reviewer
Hájek Jiří	AZD	Specification, Reviewer
Kevický Dominik	AZD	Specification, Reviewer
Matowicki Michal	AZD	Specification, Reviewer
Adrian Baron	SMO	Specification, Reviewer, Expert input
Andreas Steingröver	SMO	Specification, Reviewer, Expert input
Markus Korb	SMO	Specification, Reviewer, Expert input
Thomas Schnapka	SMO	Specification, Reviewer, Expert input
Angel Fernandez Gago	ADIF	Specification, Reviewer, Expert input
Roger Idrovo Urgilés	CEIT	Specification, Reviewer, Expert input
Sergio Arana	CEIT	Specification, Reviewer, Expert input
Dr. Annika Dreßler	DLR	Specification, Reviewer
Benjamin Wyss	SBB	Reviewer, Expert input
Mourad Lakhili	Alstom	Reviewer, Expert input
Tahereh Fala	Alstom	Reviewer, Expert input
Olga Frank	DB	Reviewer, Expert input
Sergio Quindas Garcia	DB Netz	Reviewer, Expert input
Mikel Labayen	CAF	Reviewer
Lefevre Fabien	HRSTS	Reviewer
Giuseppe Pagliarulo	MERMEC	Reviewer
Sebastiaan Linssen	NS	Reviewer
Tom Jansen	NS	Reviewer
Saro Thiyagarajan	FT	Reviewer

Olink, H.H.	ProRail	Reviewer
Allard Katstra	ProRail	Reviewer
Geir Hansen	NRD	Reviewer
Diego Garcia Vaquero	RENFE	Reviewer
Lucía Blanco Pacios	INECO	Reviewer
Martin Kaiser	DB Cargo	Reviewer
Francisco Haro Fortes	RENFE	Reviewer

EXECUTIVE SUMMARY

The activities related to Remote Driving described in this document are linked to the task 5.4 of WP5 of R2DATO project and are in line with the R2DATO Grant Agreement. The activities carried out during the task 5.4 meetings have been reported in the document and represent the macro areas into which the current document is divided.

What was shared during the activities of task 5.4 is related to when the Remote Driver must actively intervene, when in the absence of a driver in the cabin, situations must be resolved that would otherwise block the train on the track. Situations in which the Remote Driver can take control of the train to drive the train even in normal situations were also taken into consideration.

The previous projects X2Rail-4 and TAURO have permitted to craft an architecture for the autonomous train. The findings from past projects necessitate conducting an operational analysis to resolve any lingering ambiguities. This provides task 5.4 with an important and valid starting point for further analysis of the Remote Driving issues. Before starting with the use case writing activities, the operational aspects in which the Remote Driver can improve the service were identified. Some of these areas of intervention have been shared with the other tasks of WP5. The priorities for drawing up the use cases were also identified, and they were distributed among the various partners.

An important aspect is that to the knowledge of all the partners involved in task 5.4, there is no set of use cases like the one currently produced for Remote Driving. There are only a few and barely applicable to other signalling systems different to ETCS/ERTMS. This activity therefore plays a significant role within the R2DATO project.

This Deliverable tries to set out, although not definitively, the first architectural contexts that arise from the assumptions made during the meetings.

One of the concepts highlighted is that the Remote Driver of the remote supervision centre intervenes, taking full control of the train, in the event of degradation of the automation system. But he/she also carries out normal functions not yet covered. For example, taking the train from the depot to the station when the automation is not ready to do so, or carrying out manoeuvres in the yard controlled by an operator who operates outside the train in proximity to it.

As a first step, the use cases were created independently, using a shared template. In a second step, the use cases were reviewed by partner peers in order to have better harmonization. In parallel, the file that would host them, the skeleton of this document, was created.

To make the structure and references more readable and uniform, the operating states of the remote control and the functional conditions for switching from one state to another have been identified. Together with the creation of the use cases, this was one of the most important works of task 5.4.

Subsequently, all the use cases were inserted into a single file, in which the main characteristics that are intended to be managed were indicated for each use case family.

Therefore, most of the use cases produced, concern management of the train by a Remote Driver in the RSC, but there are also those related to Remote Driving of the train by a Remote Driver who is close to the train, this usually takes place within a depot. For this reason, the interfacing aspects of the Remote Driver have been identified to characterize all the interfaces necessary for the system.

Different levels of activity on the part of the remote train driver were also identified, starting from the simple observation of what is happening up to having full control of the train.

In the same way, the transitions between the different operating modes were highlighted, indicating, to increase understanding, some physical events such as pressing a button to indicate the activation of a specific function.

In degraded scenarios, remote driver management becomes essential and sometime requires the contribution of the IMs. The degraded condition explored were in both on-board train systems and trackside systems.

Furthermore, the different levels of engagement on the part of the Remote Driver have been identified. In the end a significant number of use cases (47) was produced as indicated above for normal and degraded conditions.

All the objectives foreseen in [GA] for task 5.4 were carried out within the scheduled time. This represents an excellent result considering that the group of partners also had to align on the meaning of operation aspects associated with Remote Driving reported in section 2.5.

In conclusion, this document provides a valid starting point for requirements specification activities R2DATO WP6 task 6.7 and task 6.8 and then moving on to the subsequent implementation of a prototype.

This document focuses mainly on freight trains running in the rail network and therefore does not cover all the possible automation processes in freight yards.

In the FP5 project all areas of the FDFTO are covered. In the future there should be an alignment activity between the two projects (FP2 and FP5) to have aligned solutions.

ABBREVIATIONS AND ACRONYMS

AD	ETCS Automatic Driving Mode
ADM	Automatic Driving Module (X2Rail-4 for ATO-OB)
APM	Automatic Processing Module (X2Rail-4 component)
ARCC	Automated Rail Cargo Consortium
ATB	Automatische treinbeïnvloeding
ATO	Automatic Train Operation
ATP	Automatic Train Protection
AŽD	Project partner Automatizace železniční dopravy Praha
CCTV	Closed Circuit TeleVision
CMD	Command Message
DAS	Driver Assistance System
DLR	Project Partner German Aerospace Centre (Dt. Zentrum für Luft- und Raumfahrt)
DMI	Driver Machine Interface
EBI	Emergency Braking Intervention
ERJU	European Railway Joint Undertaking
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
EVC	European Vital Computer
FA2	Flagship Area 2
FA5	Flagship Area 5
FDFTO	FullDigital Freight Train Operations
FMS	Fleet Management System
FS	ETCS Full Supervision Mode

GA	Grant Agreement
GoA1	Grade of Automation 1
GoA2	Grade of Automation 2
GoA3	Grade of Automation 3
GoA4	Grade of Automation 4
HMI	Human Machine Interface
HITACHI	Project partner Hitachi Rail Signalling and Transportation Systems
ID	Identifier
IIM	Infrastructure Incident Manager
IM	Infrastructure Manager
IOM	Infrastructure Operations Manager
IP	Internet Protocol
ISM	Incident Solving Manager X2Rail-4 component, corresponds to R2DATO's Incident Management System
IT	Information Technology
JU	Joint Undertaking
L2	ETCS Level 2
LOP	List of Open Points
LX	Level-Crossing.
Mx	Mont x in the project.
MA	Movement Authority
MNT	Maintenance
MRSP	Most Restrictive Speed Profile
MS1	Milestone: consolidation of external inputs
OAS	On-board Automation System
OB	On-board

ODR	On-board Driver
OS	ETCS On Sight Mode
PC	Personal Computer
PD	Pedestrian Driver (see actors in section 3.1)
PD1	Pedestrian Driver 1
PD2	Pedestrian Driver 2
PER	PERception
PRDR	Pedestrian or Remote Driver.
R2DATO	FP2 project Rail to Digital automated up to Autonomous Train Operation
RBC	Radio Block Centre
RC	Remote Control
RD1	Remote Driver 1
RD2	Remote Driver 2
RODR2	Remote or On-board Driver 2
RSC	Remote Supervision Centre
RTO	Remote Train Operation
RU	Railway Undertaking
RUS	Railway Undertaking Supervisor
S2R	Shift2Rail
SBB	Project Partner Schweizerische Bundesbahnen
SF	ETCS System Failure Mode
SH	ETCS Shunting Mode
SIL	Safety Integrity Level according to [EN50126]
SIL2	Safety Integrity Level 2 according to [EN50126]
SIL4	Safety Integrity Level 4 according to [EN50126]
SMO	Project partner Siemens Mobility

SP	System Pillar
SR	ETCS Staff Responsible Mode
SRDC	Specification of the Remote Driving and Command
SRS	System Requirement Specification
TAS	Trackside Automation System
TAURO	European project: Technologies for the AUtonomous Rail Operations
TCMS	Train Control and Management System
TS	Trackside
UC	Use case
WP	Work-package
WP5	R2DATO work-package 5, Automation Processes use cases and user requirements
WP6	R2DATO work-package 6, Automation Processes Specifications

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF USE CASES

1 INTRODUCTION

The objective of task 5.4 “Definition of use cases, operational parameters and scenarios for Remote Driving” is to collect a congruent set of use cases which then allows the implementation of the subsequent activities which are the definition of the requirements and the architecture of the system. In this regard, within task 5.4, results from previous projects at a European level were also collected.

It is known to all partners involved in task 5.4 activity, that there is no set of use cases like the one currently produced for Remote Driving. What exists is a less significant set and it is not fully applied to ERTMS/ETCS. This activity therefore plays a significant role within the R2DATO project.

What is described in the document is the result of the activities carried out in task 5.4 in collaboration with R2DATO WP5 task 5.1. One goal of this collaboration was to avoid overlap between those two tasks as much as possible.

One of the important aspects that characterized the first activities was to align all partners on the same perception of how and when the Remote Driver should intervene to directly carry out actions. This affected the first months of the task's activity but allowed all partners to be aligned on the operational aspects which are then expressed in the document.

In this context, the activities of task 5.4 related to remote control were analysed starting from what had already been done in previous projects (TAURO, ARCC, X2Rail-4). The documents from these projects were analysed and the results were the identification of the operational aspects which then form the basis for the creation of the use cases. The operational areas that were extracted from this analysis are the main chapters of the document in which there are specializations of the operational area. Following this approach, it was assumed to be easily accessible for reading and consultation by interested people. The main areas are reported in Table 1. Similarly, any use cases produced for Remote Driving were also incorporated into their development and updated to reflect the evolution introduced by the activities carried out.

The innovative aspect of what is produced is that it contains the management of the operating states and transitions between them, as well as the clear definition of how the transition occurs between one control area to another and how the mastership of the Remote Driver associated with a train. All these concepts refine the scenario and allow to have a complete set of use cases.

The process followed led to the identification of the normal operating conditions and those in degraded conditions which are explicitly expressed in the chapter titles. The degraded conditions in which intervention by the Remote Driver has been envisaged are:

- Degraded modes of the autonomous train which include, in addition to malfunctions of the automation part (ATO FOR APM), also degraded modes of the ETCS system;
- Degraded modes specific to remote control which covers the faults due to some poor functioning of the connection between the supervision centre and the train or malfunctions of sensors on-board the train.

During the drafting activities of the document, it was necessary to define fixed points in the process such as the transition between the different operating states and the definition of speed management in case of poor visibility. This made it possible to standardize the description of the use cases produced by task 5.4.

1.1 SCOPE

This document constitutes the Deliverable D5.4 “Documentation of use cases for Remote Driving” of task 5.4 in the framework of the WP5 of FP2 R2DATO.

1.1 PURPOSE

The purpose of this document is to provide a solid basis of description and use cases that will be the basis for future developments, starting from the definition of the architecture and functional requirements.

The main purpose of current use case collection is to propose a basis for test, validation and further improvement in R2DATO’s demonstrator projects:

- an ergonomic concept about responsibility handover between drivers.
- a list of driving situations, sketching the expectations to remote control, either with ATO or not expected behaviours while protection degrades: ATP, obstacle avoidance.
- a set of train behaviours preparing safety concepts – when visibility degrades for the remote driver.

The output of task 5.4 is relevant for the WP6 activities.

1.2 DOCUMENT STRUCTURE

In chapter 3, p.26. the Operational Assumptions common to the use cases are introduced, where the operational aspects related to remote control are defined.

Subsequently, the use cases are gathered in three parts, and each part has some related chapters- see Table 1 below.

Finally, chapter 13 p.154 introduces the conclusions. It describes current status and sketches some outlook on remote control.

	Chapter	Title	Description
General Description	2	Development Methodology	Describes the activities performed to generate this document
	3	Operational Assumptions	Defines the operational aspects related to remote control.
	4	Result Overview	Contains an overview of all use-case in this document.
Start and Hand-Over	5	Connection Between Train And Remote Supervision Centre	Defines the registration of a train at some RSC
	6	Bringing A Train To Operations	Contains the typical use cases in which a Remote Driver monitors a train.
	7	Negotiate Mastership	Contains exemplary use cases about the mastership-negotiation between on-board drivers, Remote Drivers and pedestrian drivers.
Operations	8	Driving	Contains all use cases describing nominal behaviour activities.
	9	Pedestrian Driver	Describes operations for a Remote Driver near the train.
	10	Transverse Topics	Contains operations that are present in any typical condition – driver vitality check, sounding the horn.
Degraded Operations	11	Addressing Degraded Modes of the Autonomous Train	Contains use cases in the event of a failure in the automation system.
	12	Degraded Modes Specific to Remote Control	Describes operations while some fault occurs in the process chains of the remote control itself.
	13	Conclusions	Describes where we are and sketches some outlook for remote control.

Table 1: Document structure

1.2 LIMITATIONS

The contents in this document are a basis for future human machine integration and safety analyses. They do not replace them because the assumption that there is a human figure who supervises the correct functioning of the system remains valid.

Descoped use cases and refinements out of the scope of current document are documented in Appendix 1, p. 157.

2 DEVELOPMENT METHODOLOGY

In this section, the methodology on how this deliverable was developed is discussed. The methodology section is split out in five sections:

- Deliverable objectives;
- Process overview;
- Existing and relevant deliverables;
- Methodology for use case Development;
- Definition of Operational Scenario.

2.1 DELIVERABLE OBJECTIVES

This deliverable is created on the basis of the guidelines as described in the Grant Agreement [GA]:

"Task 5.4: Definition of use cases, operational parameters and scenarios for Remote Driving (Leader: MERMEC) Participants: AZD, ADIF, CAF, HITACHI, SMO, GTSD, DB, CEIT, SBB, NRD, NS, PRORAIL, DLR, FT, ATSA) (Duration: M3 to M12)

1. *First activity will consist in collecting and analysing existing and relevant deliverables from partner projects. Relevant functions, related use cases and operational scenarios will be collected. The starting point will be the Shift2Rail projects TAURO and ARCC.*
2. *The use cases and scenarios (operational layer) will be defined in cooperation with System Pillar (SP) (first input from System Pillar is necessary) for:*
3. *Remote wake up;*
4. *Remote control operations (e.g., HV enabling, Diagnosis operations - in cooperation with TE1);*
5. *Remote Driving strategies (e.g., remote speed regulation, Remote GoA2, Initiation of GoA4 driving); Handling relevant degraded situations and shunting operations (input from FA5 is necessary);*
6. *Freight specific use cases for remote supervision & driving (input from FA5 is necessary);*
7. *Inputs from the SP, Flagship Areas 5 and 6 will be considered until M6 (MS1 – Consolidation of external inputs milestone).*
8. *Resulting use cases will cover both operational and functional aspects."*

On basis of the description that was provided in the [GA], the following can be concluded that are propaedeutic for the creation of the D5.4:

1. Relevant input from partner projects (X2Rail-4, ARCC and TAURO, other FAs and SP) needs to be collected, analysed and if relevant, included in the deliverable. Input from these partner projects will be considered until month 6, June 2023, of the project.
2. Task 5.4 will create an overview of the operational functions that are currently performed by the driver, which will be performed by the Remote Driver.
3. Task 5.4 will develop use cases for "Remote Driving functions" for Passenger and freight trains. This will be done in cooperation with the SP if input is received before month 6.

2.2 PROCESS OVERVIEW

Following figure gives an overview of the works of task 5.4:

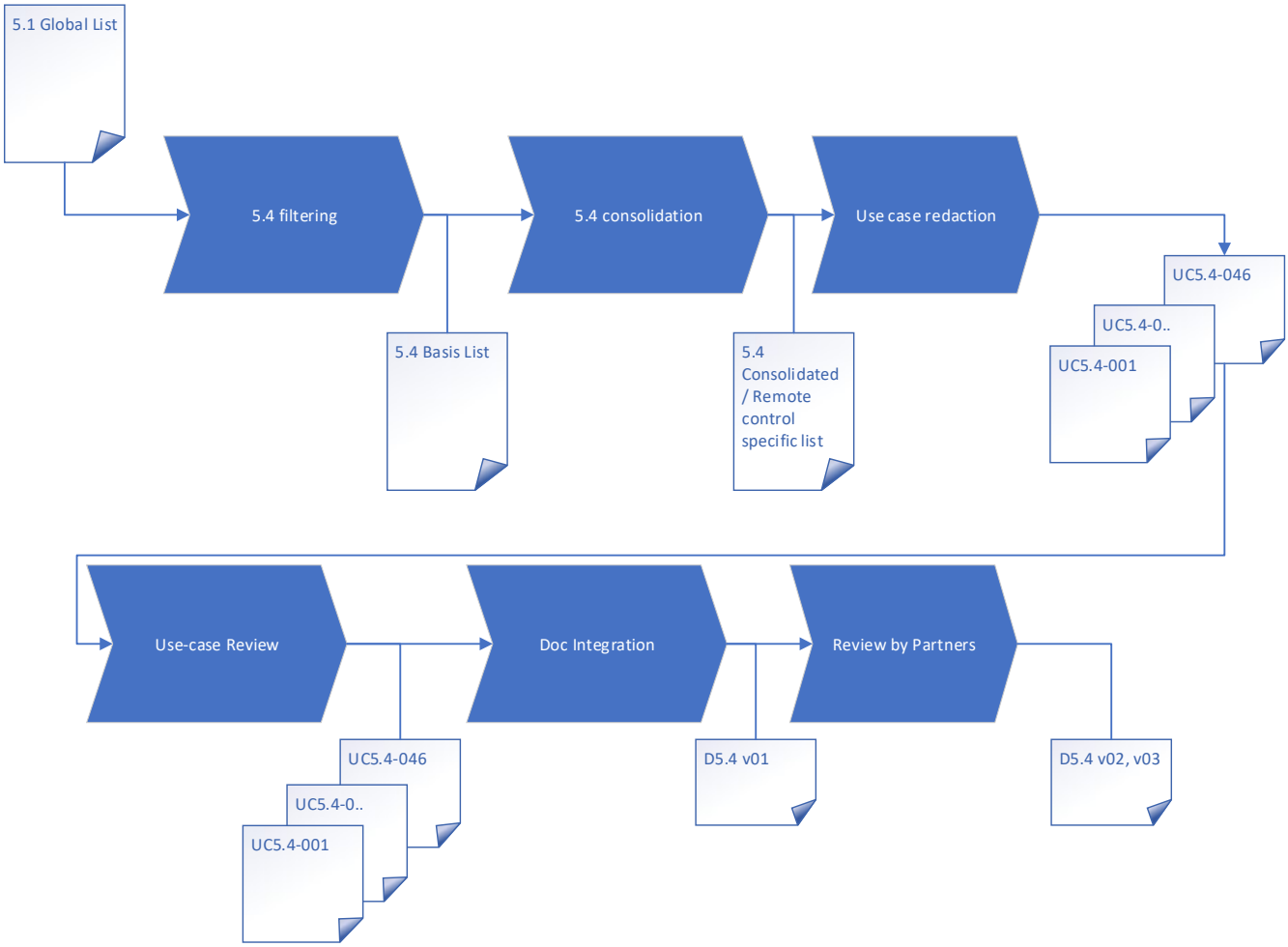

Figure 1: Task 5.4 detailed works

2.3 EXISTING AND RELEVANT DELIVERABLES

As input to the Work Package 5 process, the state of the art was considered and deliverables from past projects were identified and actively requested at the Work Package level. For this process, inputs were collected from several relevant projects:

Shift2Rail – IPX - TAURO 1st Release package (transfer date 06/02/2023)

Shift2Rail – IPX - TAURO 2nd Release package (transfer date 31/05/2023)

Shift2Rail – IP2 - X2Rail-4 Baseline 0 (transfer date 05/05/2023)

Shift2Rail – IP2 - X2Rail-4 Baseline 0.1 (transfer date 23/06/2023)

Shift2Rail - IP5 - ARCC Demonstrator – Deliverable 1.7 “Documentation and evaluation of GoA2 freight demonstrator test results in specified testing scenarios, proposal of next steps” (downloaded from project website 30/01/2023)

Due to the delay in receiving formal inputs compared to the input deadline of M6, some intermediate deliverables were requested and delivered on relevant topics for WP5.

To avoid further delay and ensure a viable result before the deadline M12 of WP5, the work package team started work on the basis of these intermediate deliverable and draft documents, establishing the potential gap with the intended WP5 results. The understanding of this gap was then used to ensure the effort within task 5.4 was focused on drafting use cases for known open topics, while avoiding duplication of use cases that would become available in Shift2Rail projects.

Once the formal deliverables became available, an analysis was performed on the delta of these deliverables compared to the inputs used for the ongoing work in the WP5 tasks. Additionally delivered use cases were processed into the use case index registering them as available input, with the specific topic of the use case no longer needing development within task 5.4.

2.4 Methodology for Use case Development

The deliverable 5.4 is one of the early deliverables inside the Automation Processes Cluster of R2DATO. This work group relied on deliverables from the Shift2Rail programs of X2Rail-4 and TAURO. In parallel, inputs were also sourced through the partners of the workgroup. These became the fundamental inputs to start the process of input collection.

The entire process described was shared and approved within task 5.4 and also at WP5 level.

The first step was to define the operational aspects in which Remote Driving should operate.

For each operational aspect, the titles of the associated use cases to be developed have been identified.

It was also analysed whether the specific use case was shared in some other tasks of WP5 to avoid overlaps. When overlaps were identified, a decision was made in which task to develop it.

At the end of these steps a list of use case was produced and was checked for redundancy.

The next step of the process was the prioritization of the use case list, with the goal to identify the right priority levels so that the available time and personnel would be effectively used to focus on describing the prioritized use cases.

Five priority levels have been identified; the priorities are linked to the level of perception of the urgency required for Remote Driving activities. The priorities answered the question of when this feature should be implemented first to meet operational needs. Each partner answered this question for each use case.

Once this set was defined, the two highest priorities were chosen which correspond (roughly) to the 47 use cases produced.

These use cases were then distributed among the partners for start the development phase.

Once the use cases were drafted, the workgroup followed a structured approach from the point of drafting the use case to finalizing the use cases with the required consensus and approval. The following 7 steps illustrate this process:

- First development stage – responsibility of the partner writing the use case.
- Review – responsibility of the partner reviewing the use case.
- Second development stage – responsibility of the partner writing the use case.
- Formal review – responsibility of the partner reviewing the use case.
- Third development stage – responsibility of the partner writing the use case.

- Finalized (stored in Cooperation Tool the Deliverable document D5.4) – responsibility of the partner writing the use case.
- Insert all the use cases in the Deliverable document.

As can be seen in the process described, it required a good collaboration among the partners for writing and reviewing the use cases before agreeing on the finalized use cases.

2.5 Definition Of Operational Scenarios

This section describes the process that led to the definition of the operational scenarios adopted in Deliverable D5.4.

In task 5.4 the activity started, first by analysing the work done in other projects and then by defining the areas of degradation in which the Remote Driver becomes fundamental if there is no Driver in the cabin. As a first step, task 5.4 starts to answer at the questions:

- Which scenarios have been analysed in TAURO and X2RAIL-4?
- When does the Remote Driver typically take over driving the train?

The analysis of the responses provided by the involved partners first made it possible to align everyone on the meaning attributed to Remote Driving. The next step was to identify the operational areas within task 5.4, the following first list was consolidated.

Connect remotely (not taking ownership yet)
Negotiate responsibility for train.
Negotiate train responsibility during shunting.
Redirect telephone calls
Start motion +Immobilize loc while climbing on it
Passenger train Coupling/Decoupling
Drive Remotely
Passenger and Freight
Any use-case where the driver relies on sound
Any use-case where the driver relies on its acceleration feeling.
GoA2 doesn't work.
'GoA2 + ETCS doesn't work.
Video flow getting too low.
Monitor remotely driven train.
Joining
Remote driving performed by a distant driver.
Remote driving performed by an on-site driver.
The remote driver is no longer able (for whatever reason) to drive a train.
Remote warning.

Table 2: First list of Operational Scenarios

During the subsequent meetings of task 5.4, the actual need to adopt the scenarios indicated in the first list was assessed and a consolidation of the scenarios was carried out.

At the end of the process, agreement was reached on the following list, which is adopted in the document. The Table 3 reports these Operational Scenarios.

Wake up, Switch on/off a train
Register and unregister a train on RCC
Logging on standby train
Take control of a train
Remote ETCS Start Of Mission
Logging on a train in operation
Loggin off a standby train
Negotiate Mastership
Hand-over between Driver and Remote Driver
Hand Over between Remote Drivers
Hand Over from/to Autonomous Train
Driving in normal condition
Driving from yard to platform and vice versa
Depot Manoeuvres
Shunting Yards
Pedestrian Driving
Degraded mode of Autonomous Train
• Degraded ATO
• Degraded Perception
• Degraded APM
• Degraded ATP ETCS on Board
• Wayside Signalling System out of order
Degraded mode of Remote Control
• poor visibility due to weather
• poor up-link connection
• Loose Its Track Sensors
• poor down-link connection

Table 3: Consolidate list of Operational Scenarios

3 OPERATIONAL ASSUMPTIONS

This chapter presents the assumptions underlying the use case definitions in this document. The defined concepts shall be considered under following light:

HMI aspects: a very simple concept is proposed, inspired by the ATO-Engage button. The intent is that this concept can be validated i.e., also rebutted and replaced by a better proposal.

States: some states and their transitions were proposed, with the purpose to elicit how operational actors RSC, train and Remote Driver interact with each other. Again, minimal state machines were preferred. In any case, attention was given to maintain the state machines as independent from each other as possible (describing the relationship of two actors to the exclusion of others). This minimality intends to support verification and challenging i.e., these states and their transitions may be improved from WP6 on.

Distances and times: a similar spirit led to the elicitation of times and distances proposing concrete visions to enable improvement (early fail philosophy).

These definitions are proposed to help describe the use cases in a concrete way.

They shall be refined in R2DATO WP6 task 6.7.

3.1 OPERATIONAL ENTITIES AND ACTORS

The following operational entities are considered:

Remote Supervision Centre, abbreviated RSC: the organization implementing the remote control of trains in the use cases of this document, including facility and IT environment. It deals with the various remote activities some RU has with its trains. The remote connection between train and centre can be triggered by both sides (see Chapter 5 p.56). According to the situation, the users in the centre can monitor or take control of the trains (Chapter 6 p.63).

The RSC can be operated by a railway undertaking. However, it is not mandatory. For instance, when a train enters a shunting yard, it may be taken over by a driver belonging to the yard, the yard's infrastructure manager now acting as railway undertaking.

Train as organisation: the train including its physical load and automation, seen as participant of the railway process (process: object of journey and MA, physical: moving along rail)

Serviceable train: physical train unit plus the parts of the train that allows human users to access the physical train unit while controlling the train (see section 3.2.2 p.29 about driver states)

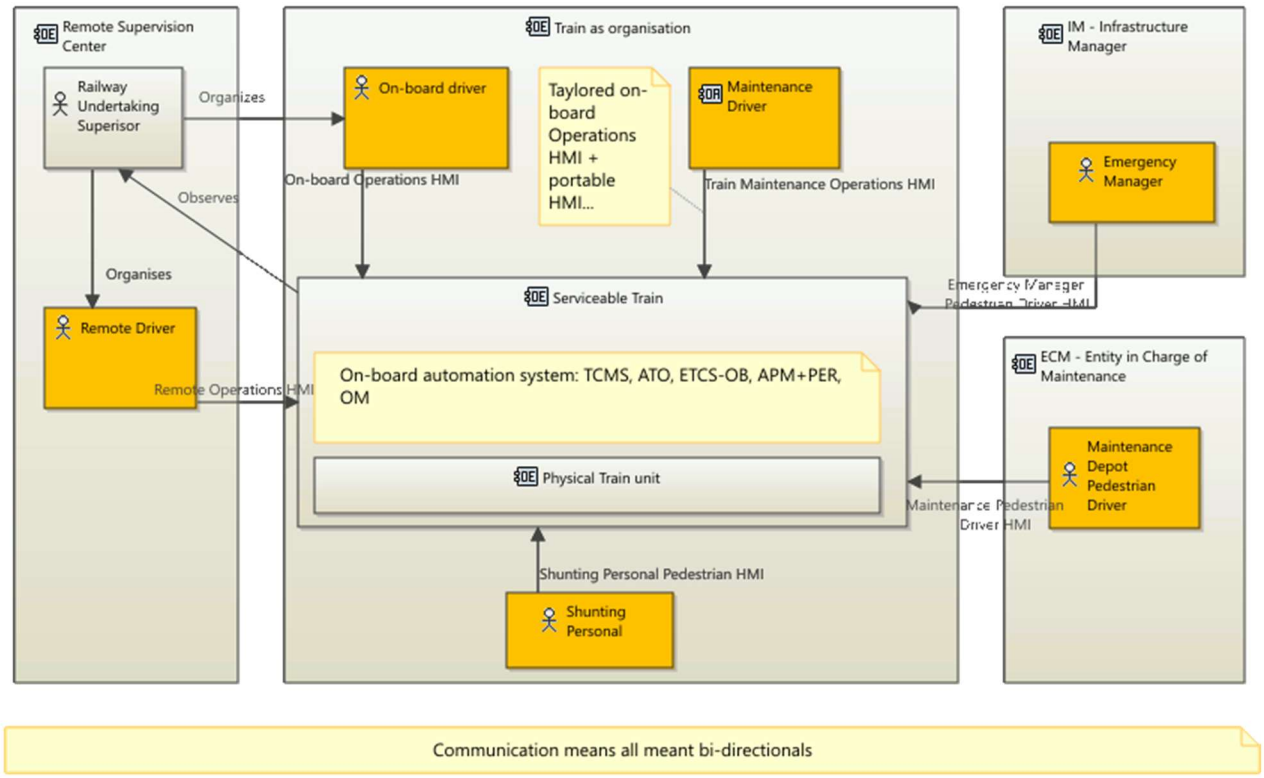

Figure 2: Operational entities and actors directly involved in remote control.

The following operational actors are directly involved:

On-board driver: Person belonging to the Railway Undertaking mandating the train, located in the train's front cabin, and driving the train manually of by means of ATO (GoA2).

Remote Driver: as identical in its role to the on-board driver as possible but located in the Remote operations facility, the remote supervision centre. Remote driver may monitor or control a train. For the responsibility (control) to be passed from one driver to the other, handovers are foreseen (section 7.1.1 p.83 and 7.2.3 p.92)

The operational functions performed by a remote driver, like an onboard driver, in this document are detailed in section 3.2.2 p.29.

Pedestrian Driver: somebody controlling the train from its close vicinity. This person may be an Emergency Manager ([SRS X2Rail-4 v0.3.0], §9.4) moving the train in case of an emergency, some shunting personnel (section 8.4 p.114) or some maintenance-depot pedestrian driver: a pedestrian in a Maintenance yard who is moving the train.

For some manoeuvres, a pedestrian driver at each extremity of the train may take control of the train closely after each other.

Following operational actors are referred to: [SRS X2Rail-4 v0.3.0]'s railway undertaking supervisor appears in the use-cases coordinating the drivers. Towards the train, his/her role remains Observing or Monitoring the train – see definition in section 3.2.2 p.29). This means that if a RUS starts Controlling a train (section 3.2.2 p.29), he/she is no longer considered RUS. He/she has changed role and, in this document, has become a Remote Driver. All the actors that are not expressly mentioned in this paragraph are aligned with those indicated in R2DATO WP5 task 5.1.

3.2 STATES

Some states of operational relevance are elicited commonly to all use cases. They always qualify one and only one operational actor or entity.

3.2.1 Train Registration Towards Remote Supervision Centres

A train can have, including but not limited to, the following status towards remote supervision centres:

Unregistered train: Train is unregistered at a remote supervision centre if it is not provided for observation to the drivers of the centre. A train may be deemed 'unregistered' without specification of the remote supervision centre. It means the train is not registered at any centre at all.

Registering: Registering is a temporary status of the registering dialog. While registering, a train offers the same services as an unregistered train.

Registered train: A train is registered at a remote supervision centre if the centre counts it in its list of trains made available to the drivers of the centre. A train can register at several remote supervision centres at a time.

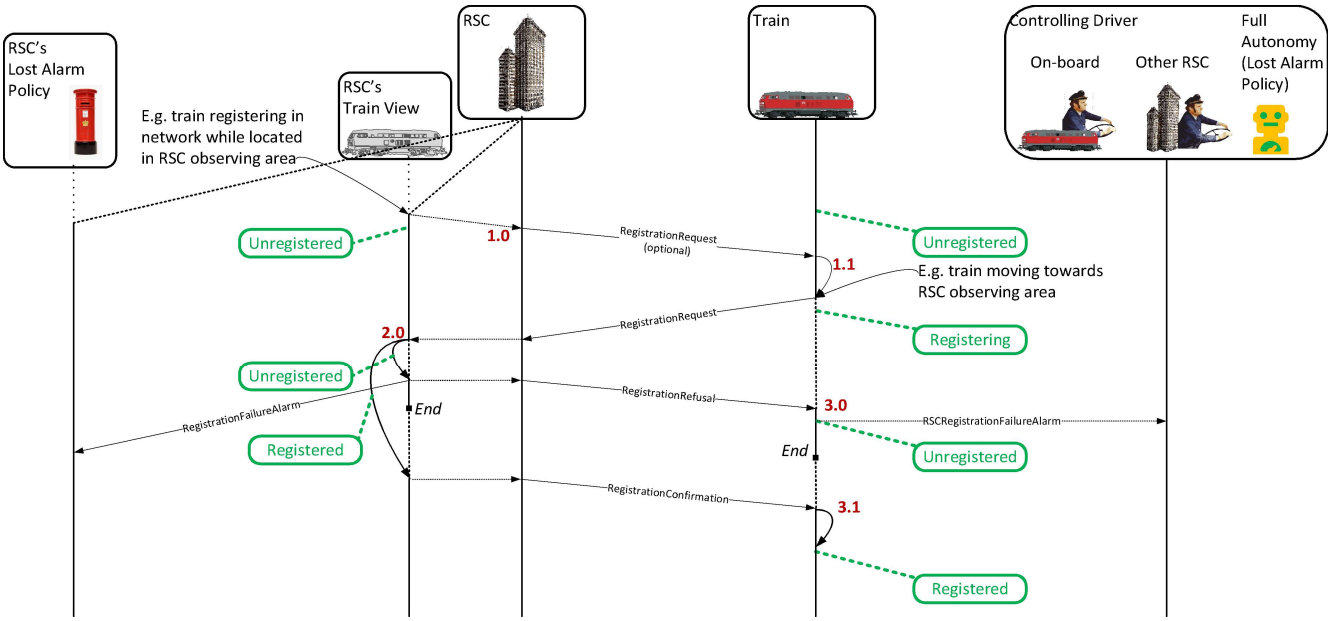

Figure 3: Train registration dialog

Once registered at a centre, the train automatically shares with the centre its observation information. This information is then provided to all users of the centre that may need it: some RU-Supervisor allocating a train to a driver, a driver needing to choose a train for monitoring. The observation information comprises:

- Other registered centres,
- Current GoA Level,
- Monitoring drivers in each centre, or at least their number.
- Driver in control of the train, also on-board.
- Level of operation (see section3.2.4 p.32)
- Position on track, speed

The centre sends to the train its *Supervision Centre Information,* useful to manage the handover from supervision centre to supervision centre (see e.g. use case *UC5.4-007)*. It comprises:

- Area of responsibility
- Neighbour centres:
  - Their Area of responsibility and
  - Contact/ network information

Note 1: a train may be registered on the network, and yet not at a remote supervision centre.

Note 2: A train may be deemed 'registered' without specification of the remote supervision centre. It means at least one centre exists, at which the train is registered.

Registration is defined in chapter 5 p.56. Several use cases tend to automatic registration so that it is seamless for the driver or possible for an autonomous train. Manual registration is also possible.

3.2.2 Driver Status Towards a Train

Once a train is registered at a remote supervision centre, the drivers managed by this centre can have, including but not limited to, the following status toward the train: Uninvolved, Observing, Monitoring, Controlling.

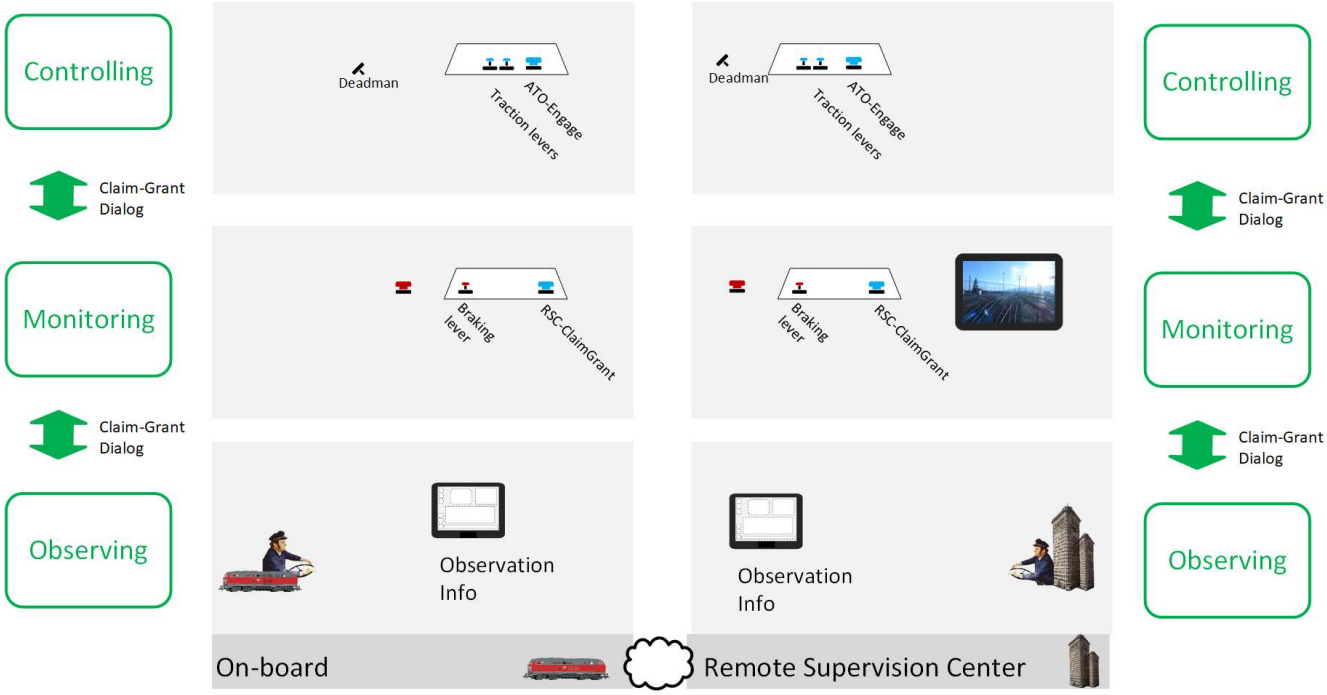

Figure 4: Driver status toward a train

They have the following meaning:

- Uninvolved: The user is neither observing, nor monitoring, nor controlling the train.
- Observing: A remote user in a remote supervision centre observes a train if:
  - He/she has no responsibility toward the train.
  - He/she gets the observation information available from the train to e.g. assess whether he/she shall/can monitor the train.

The user can also be a driver or a RU-Supervisor intending to assign the train to a driver.

Please beware:

- Any user in a registered RSC can observe a train currently controlled by an on-board driver, by another Remote Driver or running autonomously.
- The information displayed to the driver may depend on the user profile: Railway undertaking supervisor, Remote Driver in the control centre, remote pedestrian driver along the train or maintenance staff on-board.
- When a driver is Observing, he/she is not under Remote Driver vitality check (UC5.4-017).

Monitoring: A driver in a remote supervision centre monitors a train if:

He/she gets monitoring information from the train to assess it in its current state and enable a switch in "controlled". The monitoring information displayed to the driver depends on the train mode/state:

- Train operative (section 3.2.4 p.32): the full monitoring information.
- Train in standby (section 3.2.4 p.32): observation information + the part of the monitoring information that is currently available on the train.

The monitoring information is defined as:

- observation information (See p. 28)
- TCMS Information
- Video
- Sound
- ETCS, APM and TCMS Alarms

A Monitoring driver is responsible for:

- Acknowledging take-over requests by the controlling driver (remote, on-board)
- Acknowledging any request for assistance from an autonomous train – for instance if a mandatory component train loses the GoA4 readiness conditions.
- Actuating Service braking, Emergency Braking or Horn in case he/she senses that some precaution may be necessary while he/she is monitoring (but see R5 about this topic).

When a driver is Monitoring, he/she is not under Remote Driver vitality check (UC5.4-017).

- Controlling: A driver in a remote supervision centre controls a train if:
  - He/she gets all the monitoring information available from the train. He has assessed that it is enough for a safe driving.
  - He/she has access to the train control beyond the minimum emergency set available in monitoring.

  A Controlling remote driver, like an onboard driver, is responsible for:
  - Prepare train (chapter 5);
  - Manual driving – see detailed actions in UC5.4-024, like today's on-board drivers;
  - Driving with ATO – see e.g. UC5.4-021 to 023, like today's on-board drivers like today's on-board drivers;
  - Informs (UC5.4-042) or attends passengers, like today's on-board drivers (UC5.1-054, 055, ...);
  - Services the vitality monitoring/dead man (UC5.4-017);

- Handover to other driver(s), introduced also for the on-board driver (chapter 7 p.81).

Following provisions are taken, that give the controlling driver's responsibility a frame:

- The controlling driver is the only driver responsible for the train: other drivers can only perform emergency interventions.
- As such, he/she retains this responsibility until he/she agrees with a handover. (chapter 7 p.81). Emergency situations are the exception - see UC5.4-024 and R5).
- He/she cannot monitor or control other trains.
- Other trains he/she was monitoring are now stand-alone GoA4. Their alarms are not distributed according to the lost alarm policy.
- The driver is not capable to switch (control, monitor) to another train anymore.
- While interacting with colleagues, for instance the driver of a predecessor or successor train, he/she may be displayed some observing information about the other's train while interacting with a colleague. For instance, in a pop-up window related to the speaking person.
- His/her maximum speed V_Max_Driver_Max is enforced, as well as the maximum speed associated to his/her current HMI (Emergency_HMI_MaxV, MNT_Ped_HMI_MaxV, ODR_Mnt_WkPlace_MaxV, ODR_WkPlace_MaxV, RSC_WkPlce_MaxV).
- The train now monitors the video quality and latency of the driver's workplace. Chapter 12, Degraded Modes Specific to Remote Control p.141 is dedicated to this safety relevant round-trip monitoring.

Please beware:

Note 1: a driver shifting from Monitoring n trains to Controlling 1 train has to stop monitoring at least n-1 train. This apparent contradiction is addressed by Refinement R8: Monitoring multiple trains, page 159.

Note 2: Monitoring by users other that drivers: users like the RU-Supervisor may need to monitor a train. With current definition, those users lacking skills in train driving would get access to emergency braking controls or horn. This raises the question of the interaction with the driver in charge. For instance, breaking a train by mistake while climbing a hill can be very detrimental to traffic. An alternative would be to spare those controls for unskilled monitoring users. This decision goes against safety principles and may force somebody to witness an accident in the 'first person' perspective with bound hands. The authors of this document felt like experience shall be gained with the concept, incl. asking drivers and RU-Supervisors about the interactions they wish to have.

Note 3: Although Monitoring was elicited first as a sub-set of existing 'desk open', Monitoring opens the door to a fleet of autonomous train being attended by only one driver. The idea would be to provide some kind of 'multiple CCTV' screen for one Remote Driver. For instance, in a shunting yard, a remote driver may automatically be monitoring all trains available in the yard, as soon as he/she stops controlling. He/she then chooses his/her next assignment in a (coordinated) KANBAN fashion.

Multiple train monitoring raises the problem of the univocity of the communication between train and driver.

- Alarms: If the monitored trains have no controlling driver, the alarms of all trains may be directed to a single driver. It is the responsibility of the HMI designer to make sure the driver is not overstrained, especially that he/she can associate an alarm with the right train.

- Horn: If a driver detects, while monitoring several trains, conditions requiring to sound the horn, his/her HMI may not permit to associate this emergency warning with a specific train. All trains shall sound the horn. If a train is being controlled by a human driver, this driver shall get some appropriate diagnosis. This ergonomic proposal is seen only as exploratory, i.e. proposed for validation during WP6.7's human factor analysis. Please refer to refinement R8 page 159.
- Service brake: If a driver activates the service brake, a dialog may ask him/her which train shall implement this braking. As long as he/she does not answer this dialog, all monitored trains shall brake. As soon as the train is chosen, other trains shall resume automatically to their previous operations. If a train is being controlled by a human driver, this driver shall get some appropriate diagnosis.

  This ergonomic proposal is seen only as exploratory, i.e., proposed for validation during WP6.7's human factor analysis. Please refer to refinement R8 page 159.
- Emergency braking: If a driver detects, while monitoring several trains, conditions requiring some emergency braking, his/her HMI may not permit to associate this emergency braking with a specific train.

A proposal could not be defined for this document, that would be acceptable for all parties involved. Consequently, this document defines no policy for this case. Instead, R8 page 159 was issued. There, a proposal is made according to circumstances.

Those topics go beyond current document's scope. Therefore, refinement R8 was issued.

3.2.3 Train Control Status Toward Remote Drivers

A train can have following status toward Remote Drivers. For a train, being stand-alone excludes being observed, monitored or controlled, and vice-versa. A train may be observed, monitored and controlled at the same time by drivers in different RSCs.

- Stand-alone: A train is 'Stand-alone' if no remote user is currently observing, monitoring or controlling this train.
  - a stand-alone train can be registered or unregistered (section 3.1 p.26).
  - a stand-alone train may be standby or has to be fully autonomous. Operative and not autonomous is excluded by the need to enter 'monitored' or 'controlled' (section 3.1 p.26).
- Observed: A train is said observed if at least one user in a remote supervision centre observes this train.
- Monitored: A train is said monitored if at least one Remote Driver monitors the train.
- Controlled: A train is said controlled if one and only one driver in a remote supervision centre is controlling the train.

3.2.4 Train Level of Operations

[SRS X2Rail-4 v0.3.0] presents an already consolidated energy management. It introduces the terms battery protection, energy saving mode, service retention (Standby). In the following, those states are limited to that necessary under the light of remote control.

To prepare merge (WP6), a level of operation is introduced. Including but not limited to, the following modes:

- Off: A train is defined as switched off if it does not provide the minimum services of standby, and only an electric switch on will enable providing them again. For instance, the train cannot be restarted remotely: By definition, this would require standby.
- Standby: Current definition of standby is made under the strict light of remote control. it is defined by its minimal service offer: all the services necessary to register or answer positively the registration, Monitoring and control requests coming from some RSC or its drivers. It aims at being equal to X2Rail4's standby. It contains service retention.
- Operative: A train providing the services of the serviceable train, at the core of which driving capability.

Switched off:

As already arbitrated in the context of X2Rail, switched off is not considered during operations even if it may exist during the train lifecycle (e.g., assembly, retrofits, and disassembly). The reader may refer to TUM-10.1, TUM-10.2 in [SRS X2Rail v0.3.0]. The lowest level of operations considered in this document is standby.

Standby:

Some telecom component allows communication: RSC or the train can start the registration dialog.

Remote control, authentication, user profile management or system management services are necessary along the scenarios of this document implying standby, e.g., registration and Monitoring. They may not be up-and-ready yet while registration starts, hence are not necessarily part of the minimum standby state. The standby state shall be capable to activate them.

- A standby train offers the service 'switch to operative'.

About other services and merging with X2Rail-4: when an operative train is set to standby, the aim is that it saves energy. To this intend it is expected to offer limited services compared to operative. This very likely excludes services associated to operations (traction, unlocking doors, coupling, braking other than parking). This aspect is important and corresponds to X2Rail-4's 'Limited service'. Standby does not define which services are restrained, continuously or intermittently. For instance,

- Time management and temperature supervision are likely to be provided continuously.
- Slide supervision and cold movement detection are likely to be provided continuously.
- The train may retain the capability to monitor batteries and, periodically, recharge them on its catenary.
- The train may retain some door management services for a driver to board the train, as well as services to start the cabin. This is not part of the definition of standby as defined hereby. In particular, those services may be defined with other states to the convenience of the rolling-stock producer / responsibility of its design.

Operative:

Operative means at least that TCMS is up and running. Operative sets not expectations about the degraded mode a TCMS may choose to enter according to the convention in this document, the train is still operative, even if degraded.

If the responsibility of the train is not defined, i.e., no driver is controlling the train, the train stands still (unless it is running GoA4 but this is not scope of current document). The behaviour is considered safety relevant, especially if ETCS-OB is isolated.

Operative is likely to mean that ETCS is up and running. As a degraded mode, it may be isolated. See provisions about standstill when no driver controls the train.

Operative is likely to mean ATO up and running, without assumption of engagement. Operative does not require it, however.

Operative is likely to imply obstacle detection (PER and APM) is up and running. Operative, however, does not require it.

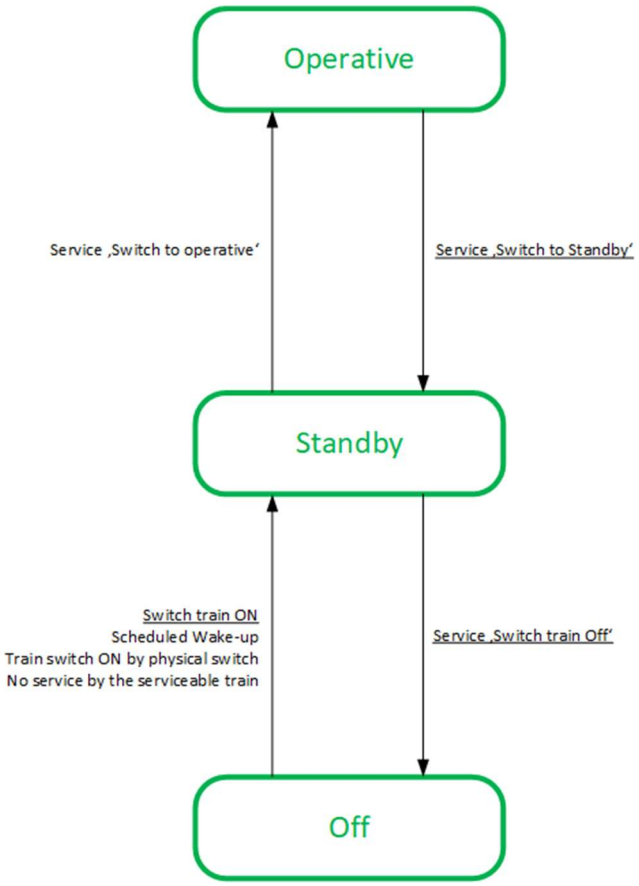

Figure 5: Levels of operations

3.3 Driver Machine Interfaces

Driver machine interfaces are taken into consideration in current document. The idea was to make emerging process concrete for both authors and readers. Authors: help generate a rich output/generate creativity by confrontation with reality. Reader: help imagine operations as real as possible, thus provide better validation freedom.

DMIs don't just help figure out processes. They also contribute to their definition by providing bottlenecks for the information actors exchange with each other. Therefore, it is important that readers keep in mind that the DMI (components) in this document are proposed for validation, a.o. in the context of WP6.7 human integration studies. Consequently, they may change. To this intend, interactions with DMI components (RSC-ClaimGrant safe push, long push) also have been defined by their meaning / process semantic.

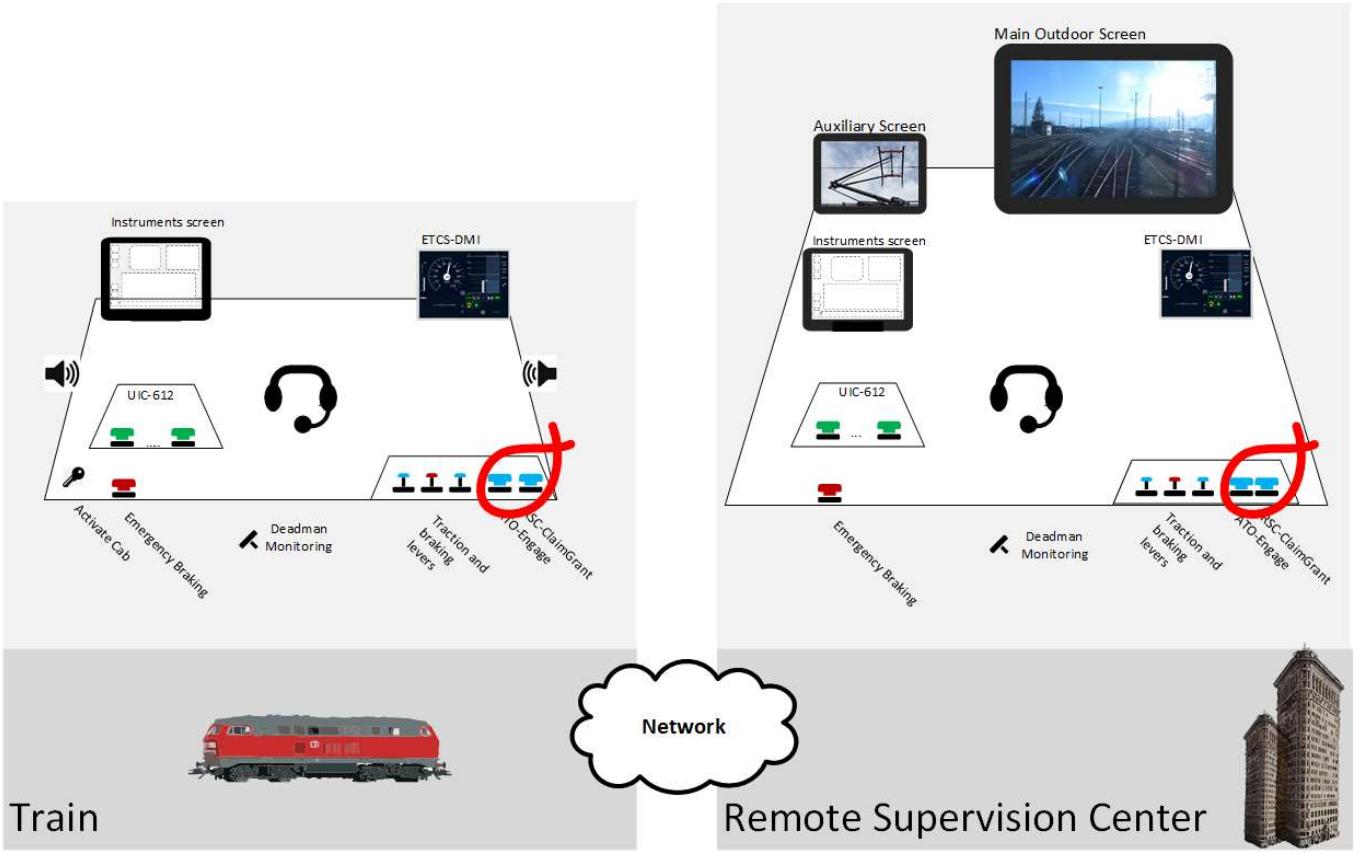

Figure 6: Remote Operations HMI

Following Driver Machine Interfaces are directly involved:

- On-board operations HMI: Driver desk in a real cabin, as usual and as shown in Figure 6 p.35.
- Remote Driver workplace: Replication of an on-board cabin in RSC, as shown in Figure 6 p.35.

Note: On this figure, an instruments screen permits to show, or control detailed, train specific, components of the train. A typical application is diagnostic. This screen corresponds to an existing state of the art in today cabs but depends on the rolling stock itself. Therefore, this screen is replicated for the remote cabin as 'expected maintenance screen'. This screen, however, is not subject of the use cases in this document (see Appendix 1).

- Emergency Manager HMI: a tablet- or smartphone-based HMI that allows the emergency manager to move the train at pedestrian speed.
- Maintenance-depot Pedestrian driver HMI: a PC, tablet- or smartphone-based HMI that allows this driver to move the train at pedestrian speed.
- Maintenance Train Operations HMI: a combination of On-board Driver Workplace and PC- or tablet-based HMI that allows a maintenance driver to control the train from its front end. The on-board driver workplace may restrict some functions (max speed) while the PC may allow others (software upgrades, enhanced maintenance, …).

For the On-board and Remote Driver workplaces, following buttons are high-lighted:

- ATO-Engage – See [SS-125].
- RSC-ClaimGrant – introduced by this document, used by drivers to negotiate control of the train.

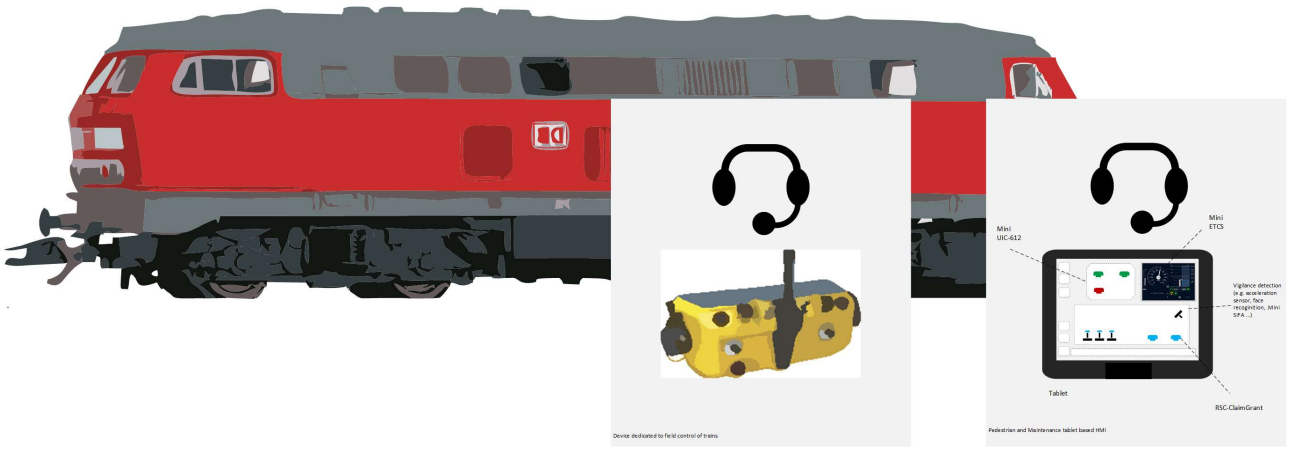

Figure 7: Pedestrian HMI for locomotive remote control

3.3.1 RSC-ClaimGrant

RSC-ClaimGrant is a button common to all HMI (on-board, remote, pedestrian) proposed in advance of Tasks 6.7 and 6.8 to concretize the document. The exact ergonomics will have to be detailed in WP6.7 (see for instance limitation R2: Safe Push, p. 158).

RSC-ClaimGrant is designed as a button used by all drivers to claim control of the train. Its consequence is changing the driver status toward the train (observing, monitoring, controlling, as defined in section 3.2.2Driver Status Towards a Train, p.29).

Actions on RSC-ClaimGrant have following meaning in this document (see Figure 8 below).

- Safe Push, shorted ‘Push’ in the document: request or confirmation of handovers to another driver, or to take-over. Originally, a single Push was foreseen. A double push was recommended, or other measures less prone to human errors. No solution emerged as the one of consensus. To keep the document simple, the document remained with ‘Push’. The need for a robust solution remains.
- Long Push: disengages driver responsibility, i.e., demotes from controlling to monitoring or from monitoring to observing – see section 3.2.2 for a detailed definition of those states. Demoting from controlling to monitoring requires acknowledgement by the train.

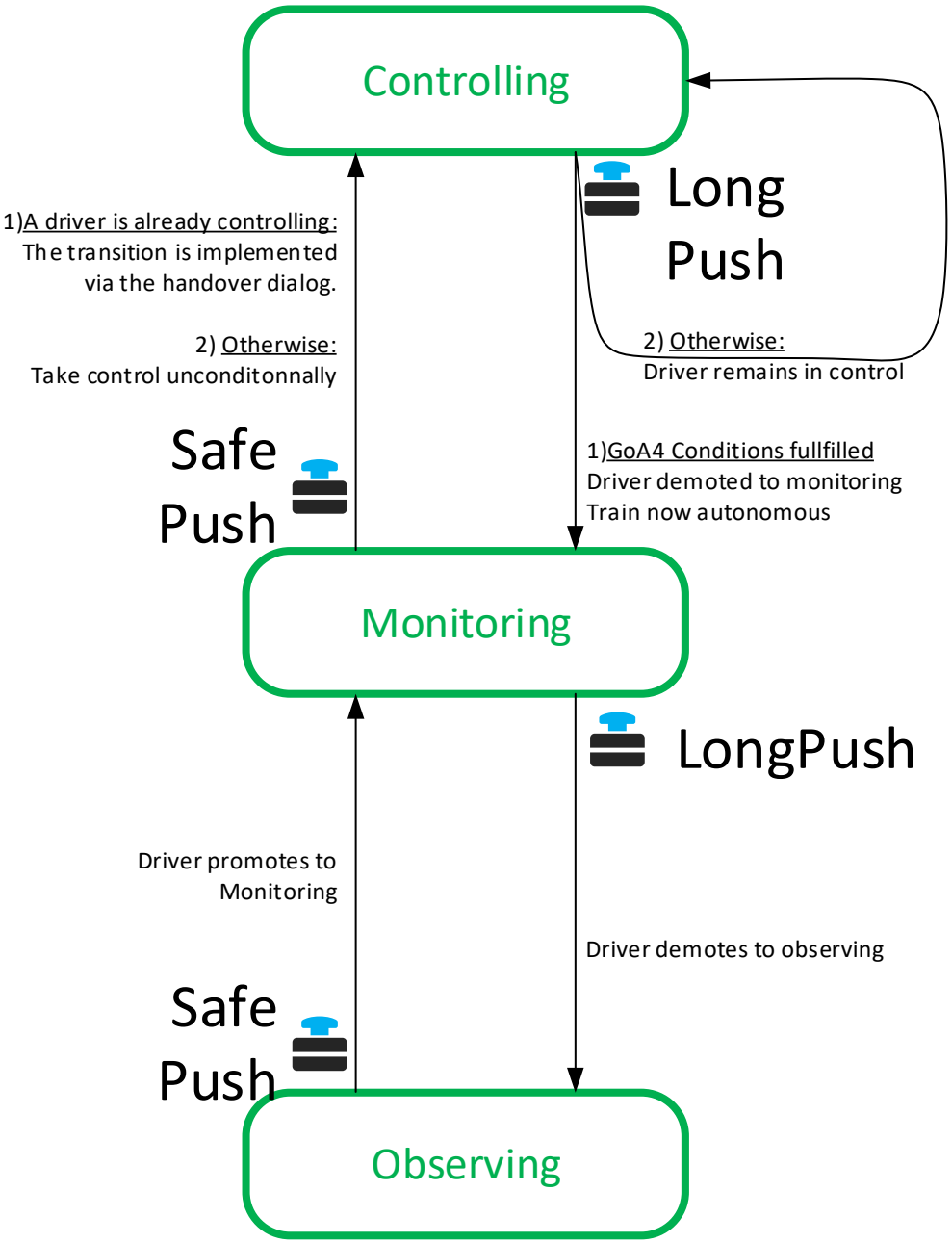

Figure 8: Switching driver status toward the train by means of RSC-ClaimGrant

Following table explains the conditions of success for demoting, and how the train may generate them if not yet available when the demoting request is issued. See also use cases UC5.4-015, UC5.4-016, UC5.4-023.

Context	Action on RSC-ClaimGrant	Meaning
Driver is Controlling No handover dialog on-going.	**Long Push**	Issues to the train a request to demote to Monitoring. The train engages ATO if not yet engaged. It checkes that the conditions for Monitored-GoA4 readiness are given, e.g. obstacle management up and running. If so, it demotes the driver to Monitoring.
Driver is Monitoring No handover dialog on-going.	**Long-Push**	Issues the train a request to exit Monitoring. The train checks • If at least one other driver is monitoring the train already, e.g. if demoting the driver will not leave the train standalone, or • If the conditions for stand-alone GoA4 are given (lost alarm policy) If so, it frees the driver from its Monitoring.

Table 2: Demoting dialog

Taking control of a train without controlling driver shall, in general, not be limited as this takeover is likely to happen while the train does not manage to run autonomously, i.e. while the traffic is already under tension (e.g., UC5.4-022). For a handover from another driver, a dialog is necessary to get his/her agreement. This behaviour is detailed in use cases UC5.4-018, UC5.4-020, UC5.4-021.

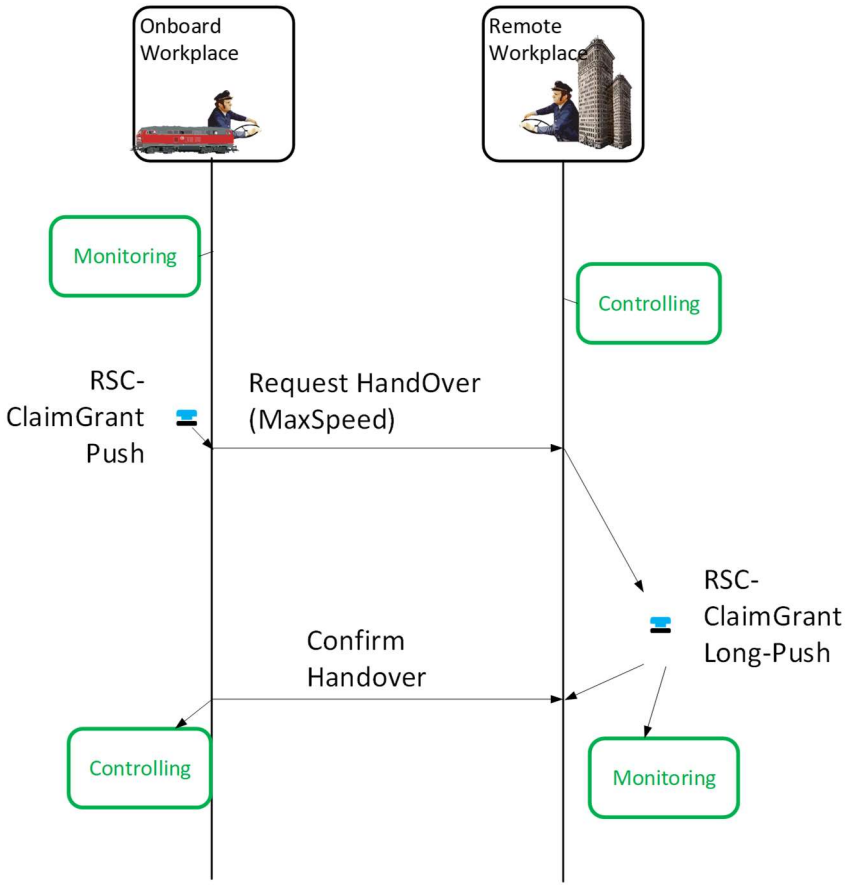

Figure 9: Successful control request initiated by on-board driver

During this dialog, the actions ‘Push’ and ‘Long Push’ are reused. This extended meaning is detailed in next table:

Context	Action on RSC-ClaimGrant	Meaning
Driver is monitoring. No handover dialog on-going yet.	**Push**	Initiate a handover dialog issue a **RemoteControlRequest** to Controlling Driver.
Driver is Controlling No handover dialog on-going yet.	**Push**	Initiates a handover dialog issue a **RemoteControlRequest** to Monitoring Driver.
Driver is Monitoring RemoteControlRequest already received.	**Push**	Issue a RemoteControlAcknowledgement to Controlling Driver. **Handover confirmed.**

Context	Action on RSC-ClaimGrant	Meaning
Driver is Controlling RemoteControlRequest already received.	**Push**	Issue a RemoteControlAcknowledgement to Monitoring Driver. **Handover confirmed**.
Handover dialog on-going: RemoteControlRequest already received.	**Long Push** by Monitoring Driver	Issue a RemoteControlRefusal to Controlling Driver. **Handover refused.**
Driver is Controlling RemoteControlRequest already received	**Long Push**	Issue a RemoteControlRefusal to Monitoring Driver. **Handover refused.**
Handover dialog on-going: RemoteControlRequest already received.	**No Push** by Monitoring Driver $T_{HandOverTimedOut}$ after RemoteControlRequest has been received.	Issue a RemoteControlRefusal to Controlling Driver. **Handover refused.**
Handover dialog on-going: RemoteControlRequest already received.	**No Push** by Monitoring Driver $\mathbf{T_{HandOverTimedOut}}$ after RemoteControlRequest has been received.	Issue a RemoteControlRefusal to Monitoring Driver. **Handover refused.**

Table 3: Handover dialog

Context	Action on RSC-ClaimGrant	Meaning
Driver is Controlling No handover dialog on-going.	**Long Push**	Issues to the train a request to demote to Monitoring. The train engages ATO if not yet engaged. It checkes that the conditions for Monitored-GoA4 readiness are given, e.g. obstacle management up and running. If so, it demotes the driver to Monitoring.

Context	Action on RSC-ClaimGrant	Meaning
Driver is Monitoring No handover dialog on-going.	**Long-Push** by Monitoring Driver	Issues the train a request to exit Monitoring. The train checks whether the conditions for stand-alone GoA4 are given (lost alarm policy), or at least one other driver is monitoring the train already, e.g. if.

Table 4: Contextual meaning of a Long Push

3.3.2 Pedestrian Warning Box

Pedestrian warning boxes are mounting on the train for pedestrian to understand the behaviour of the vehicles in their vicinity. This feature is not provided today. It is recommended (not seen mandatory) in the transition phase for trains under tests.

Pedestrian warning boxes are mounted on the train so that a pedestrian can see at least one at any time – see Figure 10.

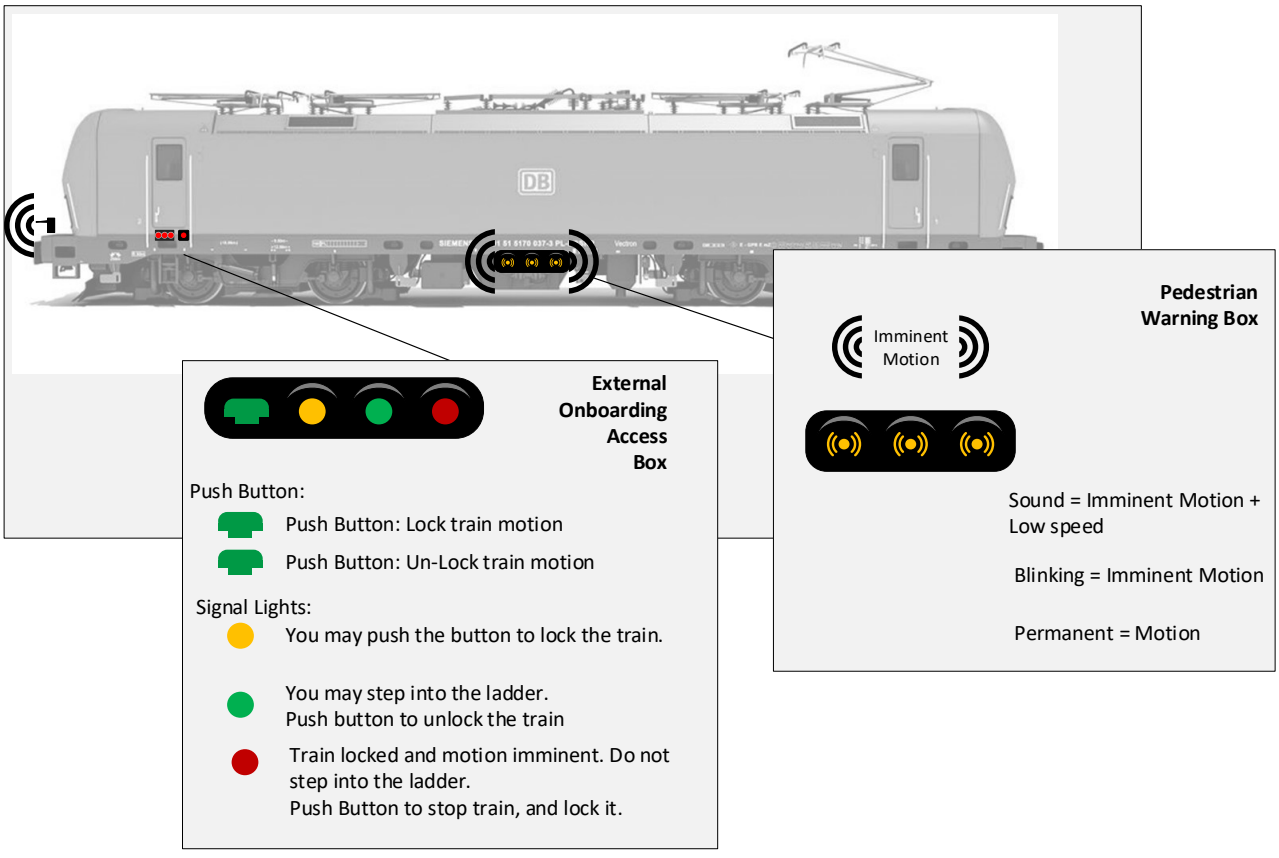

Figure 10: Pedestrian warning and On-boarding protection

As an example, before some Human Factor Analysis is performed, it is assumed that pedestrian warning boxes comprise a warning buzzer and some warning lights. They may take following states, including but not limited to:

Meaning about the train motion	Warning Buzzer	Warning lights
Standstill	Silent	Off
Imminent motion	Buzzing	Blinking. On side boxes, the blinking may indicate the direction by simulating a rotation.
Motion started (speed < 15 km/h)	Buzzing	Permanent lighting
Motion established (speed > 15 km/h)	Silent	Off

Table 5: Warning buzzer states

3.3.3 On-boarding Box

A box is assumed provided on both sides of each cabin door. Figure 10 shows the external box, for entering. An internal box helps securing the exit.

Although the function of this box can be provided differently, or in parallel of other devices (e.g. on the driver's phone), the function itself is seen mandatory to protect the health of personnel boarding or off-boarding the train.

As a proposal for its realization before some Human Factor Analysis has yet been done, following is assumed:

A 'reserve/release' button

Some lights specifying whether the train's state permits entering/exiting the train safely.

Light state	Door State	Driver behaviour	Meaning of the push-button
Off	Door available for reservation	Track: May request door Cabin: May request door	Request door for boarding
Red, permanent	Door unavailable	Track: Don't board on Cabin: Don't board off	Ignored

Light state	Door State	Driver behaviour	Meaning of the push-button
Green, permanent	Door reserved for boarding.	Track: May Board on Cabin: May Board off Both: May release door	Release door
Red, flashing	Imminent motion	Track: Keep away from train Cabin: Don't board off	Ignored

Table 6: On-boarding box states

3.4 COMMUNICATION MEANS

Following communication means are assumed in operations, although not necessarily mandatory for a demonstrator:

- Secured IP network Train-RSC: connects the remote supervision centre to the train. This means of communication supports the communication flow for the Remote Driver workplace. Includes [CYB].
- Secured IP network for Pedestrian drivers: This network supports the Pedestrian driver HMIs (emergency, maintenance). This document does not specify whether their HMI communicates with the remote supervision or with the train.

3.5 SPEEDS AND THEIR RESTRICTIONS

In general, remote control happens under the protection of ETCS-OB. Speed restrictions known in this context are enforced, consolidated in ETCS' most restrictive speed restriction. Remote control introduces new speed restrictions related to a driver's accreditation or to his/her HMI.

- V_Max_Driver_Max: Driver Maximum Speed. This speed is expected to be influenced by following elements:
  - Driver's competency profile: train attendant, full driver profile, maintenance driver.
  - Knowledge of the train
  - Accreditation for the area
  - HMI Max Speeds: For each HMI, a maximum speed is defined that defines the maximum speed the HMI allows its user(s).
- Maximum speed associated to the HMI:
  - RSC_WkPlce_MaxV: Maximum speed allowed to a driver from a Remote Driver workplace
  - Emergency_HMI_MaxV: Maximum speed allowed to a driver from some Emergency Manager HMI

- MNT_Ped_HMI_MaxV: Maximum speed allowed to a driver from a Maintenance-depot Pedestrian driver
- ODR_WkPlace_MaxV: Maximum speed allowed to a driver from some On-board operations HMI
- ODR_Mnt_WkPlace_MaxV: Maximum speed allowed to a driver from some Maintenance Train Operations HMI

For instance, a fully accredited on-board driver (V_Max_Driver_Max = 360 km/h), may be limited MNT_Ped_HMI_MaxV=5 km/h while controlling the train from the track ground.

In chapter 7 p.81 about handover, use cases foresee that the train responsibility is handed over from one driver to the other.

- For pedestrian drivers, the train has to be stopped during handover;
- For drivers in the RSC, a decreasing speed gap may exist between drivers. For instance, a full-operations driver may hand over to a driver accredited for shunting only. Specific strategies are presented.

3.6 AREAS

Chapter 5 p.56 is dedicated to the registration of trains to RSCs.

In this context, the RSC is qualified by:

- Its area of observation: the portion of the network for which the drivers of the remote supervision centre can observe trains.
- Its area of monitoring: the portion of the network for which the drivers of the remote supervision centre can monitor trains.
- Its area of control: the portion of the net for which drivers of the remote supervision centre can take control for trains.

These areas permit drivers depending on some RSC to be notified and monitor the trains (for instance the position) of the train around their area of control, prepare the control by initiating a monitoring while they approach their area or responsibility.

To enable handover between 2 drivers of different RSC, following relationships link these areas:

- The area of control of a centre shall overlap with the area of control of its neighbours. This overlap shall be long enough to enable handovers between Remote Drivers.
- The areas of a centre are included in each other: area of control ≤ area of monitoring ≤ area of observation.
- An area of monitoring wider than the area of control gives the time to a driver to prepare the control. An Area of observation wider than the area of monitoring gives the time to some RU-Supervisor to allocate Remote Drivers to newly registered trains.

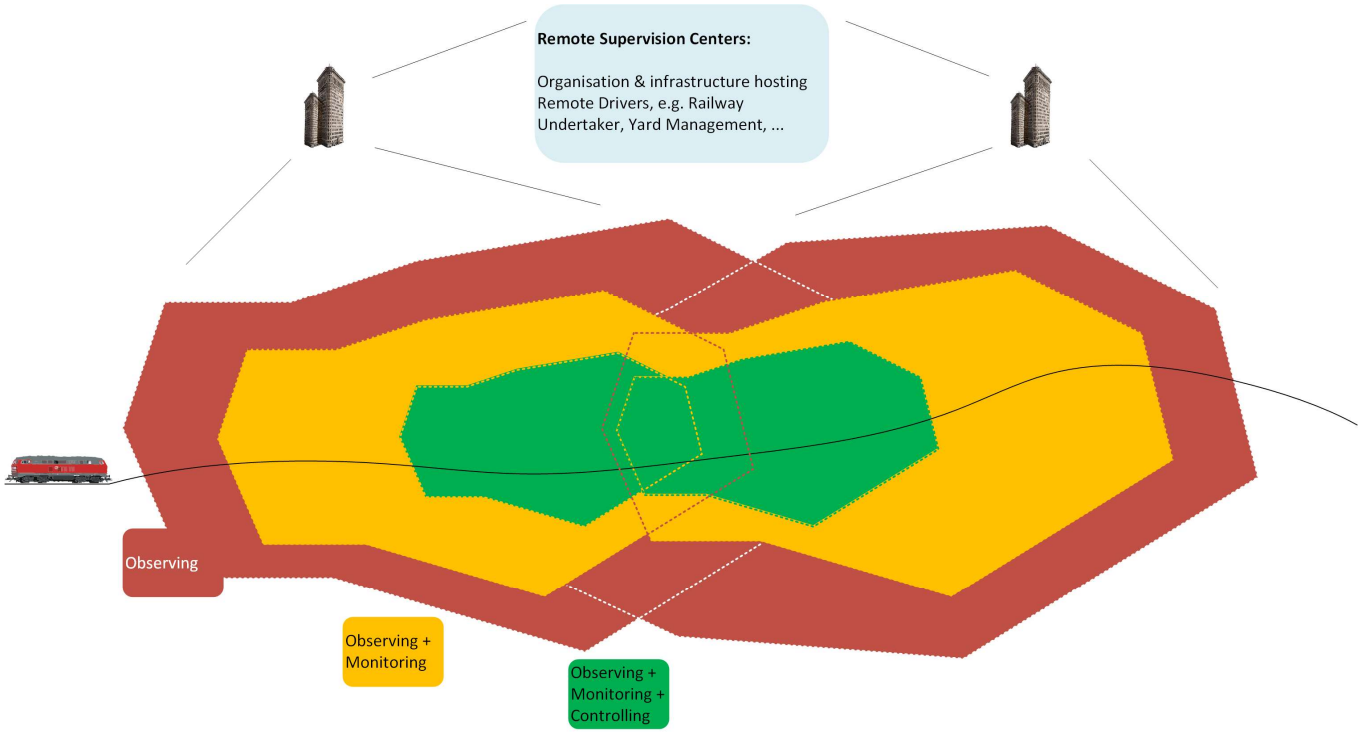

Figure 11: Areas qualifying a remote supervision centre

Note: A 'Standalone area' would be an area where the train shall not request for registration. It is the rest of the world outside the area of observation. Therefore, this area is not defined explicitly.

Refer to Chapter 5 p.56 for details.

3.7 DRIVER PROFILES

A *driver accreditation profile* is some aggregated information containing the types of driving a driver is accredited for, and where:

- Detailed driving role: Normal operations, High-speed operations, pedestrian, emergency manager, shunting personnel
- Associated max speed if any. This maximum speed may be a locally enforced national value, like ETCS's shunting max speed.
- Area of accreditation: for each accreditation role, the areas in which the accreditation is valid.

A *driver's mission profile* is the list of roles the driver currently takes during a train mission.

- Some end of accreditation if necessary, corresponding to the end of the areas of accreditation of the driver.
- Along the expected journey of the train (or movement authority), the most competent profile of the driver available at a location.
- The associated list of constant speed restrictions V_Max_Driver along the expected journey of the train.

3.8 ALARMS

Alarms are defined as messages that a train issues to its driver(s).

- They may be emitted by ETCS-OB, TCMS, ATO-OB, APM or be specific to remote control.
- While received by the HMI or workplace, these alarms may be enforced by sound, or visually, or both.
- Some alarms need acknowledgment by the driver: the proof that he/she has noticed and understood the alarm.

Alarm distribution is ruled as following

- The controlling driver, if any, is notified.
- The controlling driver, if any, is responsible for acknowledging alarms requiring it.
- The train notifies all monitoring drivers, i.e. they have access to the alarms in their history.
- Monitoring drivers acknowledge only alarms meaning that attendance is required on an otherwise autonomous train.
- If a driver is controlling, he/she only is responsible for alarm acknowledgement.
- If the train is autonomous without controlling driver, the autonomous train acknowledges the alarms that would have been directed to a controlling driver, as long as it can
- The autonomous train forwards the alarms it does not manage to process.

  For multi-train monitoring, the visual and/or sound warnings associated to the alarms of a train may be adapted. To avoid overloading drivers, the adaption should remain faithful to exiting alarm signals.

  For instance, if a driver monitoring several trains at a time focuses on one, sound warning of the alarms associated to the others may be automatically disabled by the HMI. The visual alarms may remain, incrusted in the main screen on the focused train. A dialog may be added that proposes for a short duration to change focus directly to the alarming train.

  For instance, if track-side ISM informs a train about a stuck car at a level-crossing on its way, beyond its line of sight, the driver in control (on-board or remote) will get an alarm. It the train is autonomous, and monitored by 2 drivers, none gets an alarm as the automation manages it. When the train arrives on site, it brakes autonomously if the obstacle has not vanished. It issues another alarm: as the train is overstrained, it passes this alarm to the monitoring driver(s) so at least one attends the situation.
- If an autonomous train has no Monitoring driver, the alarms of this train cannot be delivered at first. As shown by the above example, some may require human attention.

The lost alarm policy of a remote supervision centre defines how such alarms are issued to a human despite no responsible is currently allocated to the train. Following examples are given:

- The centre forwards the alarms to a Railway undertaking Supervisor.
- The centre forwards the alarms to a driver with a low workload at this moment.
- The centre rings all drivers, except those already involved in Controlling a train. The idea is that one will take control.

Defining the lost alarm policy of a remote supervision centre depends on its organisational model. Current document does not intend to set standards. As a first assumption, it assumes 1): there is always some RU-Supervisor responsible for the train until he/she has delegated reaction to alarms to some driver.

The lost alarm policy may have and influence on the train's behaviour when its last monitoring driver demotes to observing. In UC5.4.023, the train requires a responsible RUS at least. This is an operational design decision to make this use-case concrete. An autonomy-capable train may not require a permanent RUS. It requires a sound lost alarm policy, that can provide a RUS or a driver in a short time for availability reasons.

3.9 JURIDICAL RECORDING

To keep the document easy to read, steps focus of juridical recording are not always document along the use-cases. Following events have been considered.

Event	Archived by juridical recording?	Documented in use-case
Handover request	Yes	Implicit in chapter 7 p.81 about handovers
Handover refusal	Yes	Implicit in chapter 7 p.81 about handovers
Handover timeout	Yes	Implicit in chapter 7 p.81 about handovers
Changes in responsibility of drivers • See section 3.2.2 p. 29 • See chapter 7 p.81	Yes	Implicit in chapter 7 p.81 about handovers
ETCS isolation	Yes	UC5.4-041
Emergency driving actions in Monitoring Incl. forced handover if any	Yes	Implicit in UC5.4-024 Steps 3.x
Driving actions Controlling	If defined today.	Implicit in UC5.4-024 Steps 4.x

Table 7: Juridically recorded events

4 RESULT OVERVIEW

This chapter gives an overview about the use-cases in this document. Use-cases are grouped in tables, each table corresponding to a chapter in current document. The columns of those tables have following meaning:

- Id: the Use Case's unique identifier
- Name: a string describing the use case in less than 1 line
- Summary: a short description of the Use Case
- Planned GoA1-2: crossed if the use-case is relevant in the context of planned remote Go1-GoA2 operations
- GoA3-4 fall-back: crossed if the use-case is relevant as fall-back of planned GoA3-GoA4 operation

The details are within the Use Cases mentioned, described in the document in the following chapters.

4.1 CHAPTER 5: CONNECTION BETWEEN TRAIN AND REMOTE SUPERVISION CENTRE

Chapter 5 defines the registration of a train at some RSC.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-001	Register a train at an RSC	A train registers to one RSC. It ends being registered at all RSCs at which it shall be observed.	X	X
UC5.4-007	Register a moving train at an RSC	In this use case, a train detects automatically that it approaches the border of some RSCs area of observation.	X	X
UC5.4-008	Unregister a moving Train from an RSC	A train exits the area of observation of some RSC. It unregisters.	X	X

4.2 CHAPTER 6: BRINGING A TRAIN TO OPERATIONS

Chapter 6 contains the typical use cases in which a Remote Driver monitors a train.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-009	Log-in on a registered standby train	RD logs on a train initially registered and in standby. He / she is granted a monitoring access: display of train state; no control.	X	X

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-010	Take control of a monitored standby train	RD1 is monitoring a train. He/she requests its control. On success, he/she has gained control of the train.	X	X
UC5.4-011	Wake-up train by remote driver	A Remote Driver RD, already controlling a standby train (UC5.4-010), commands that it becomes operative.	X	
UC5.4-012	Switch on vehicle and prepare it by remote driver	Train wakes up (UC5.4-011), then, the driver prepares it.	X	
UC5.4-013	Perform ETCS start of mission procedure by remote driver	This use case provides remote train control operation to a driver in the RSC. The driver performs an ETCS Start of Mission procedure. After this, the Remote Driver should be able to drive the train remotely as if on the train itself. It is assumed that everything is working properly.	X	
UC5.4-014	Log-in on an operative train by remote driver	RD1, observing a train already in operations under the control of RD2, logs-in on this train. He/she ends up monitoring the train.	X	X
UC5.4-047	Demote a train from operative to standby by remote driver	On user request, the train switches from Operative to Stand-by.	X	
UC5.4-015	Demote a remote driver from controlling to monitoring	RD1 is Controlling his/her train. He/she wants to get back to Monitoring.	X	
UC5.4-016	Stop monitoring a train by a remote driver	RD1 is Monitoring his/her train. He/she wants to stop this Monitoring.	X	X

4.3 CHAPTER 7: NEGOTIATE MASTERSHIP

Chapter 7 contains exemplary use cases about the mastership-negotiation between on-board drivers, remote drivers and pedestrian drivers.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-017	Confirm remote driver vitality by remote driver	This use case details the periodic checking of Remote Driver vitality during remote train control to check attention to the screen.	X	X
UC5.4-018	Initiate handover from on-board driver by the remote driver, no ATO	RSR, monitoring a train, claims responsibility for this train. ODR, who was driving at traction chain level, grants the responsibility.	X	
UC5.4-019	Initiate handover to Remote Driver by On-board driver, no ATO	An on-board driver, controlling train, asks for handover to a remote driver already monitoring the train. The remote driver, takes the responsibility. At the end of the use case, the remote driver responds for the train while the on-board driver monitors it.	X	
UC5.4-020	Initiate handover from another Remote Driver by Remote Driver, no ATO	RD1 initially monitoring a train claims responsibility for the train. RD2, who was driving at traction chain level, grants the responsibility.	X	
UC5.4-021	Initiate handover from another driver by remote driver, ATO engaged	A Remote Driver RD1 initially monitoring a train claims responsibility for the train. A second Remote Driver RD2, who was controlling the train with engaged ATO, grants the responsibility. At the end, the RD1 is controlling the train. The train has automatically adapted its speed to RD1s maximum driving speed.	X	
UC5.4-022	Initiate handover from autonomous train by remote driver, ATO engaged	RD monitoring a train claims responsibility for the train. The train, that was driving autonomously, creates the conditions for the take-over. The take-over takes place.	X	X
UC5.4-023	Initiate handover from autonomous train by remote driver, ATO not engaged	A remote driver supervising a train hands-over responsibility for the train. The train continues driving autonomously, after verifications that it is possible. The remote driver passes the train to the attention of supervisor.	X	X

4.4 CHAPTER 8: DRIVING

Chapter 8 contains all use cases describing nominal behaviour activities.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-024	Perform routine driving by remote driver	This use case details remote train control operation by a person in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself. It is crucial that there is working communication between the train and the control centre and that the Remote Driver has working sensors based on which the Remote Driver drives and also access to warning sound devices.	X	
UC5.4-025	Move train from yard to platform by remote driver– free track	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	X	
UC5.4-026	Move train from yard to platform – occupied track	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	X	
UC5.4-027	Move train from platform to yard.	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	X	
UC5.4-028	Move the train in depot for train composition by remote driver	This use case details remote train control operation in depot by a person in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself. It is crucial that there is working communication between the train and the control centre and that the Remote Driver has working sensors based on which the Remote Driver drives and also access to warning sound devices.	X	
UC5.4-029	Shunt in centralized area	Driving the train in a centralized area (shunting). The train is driven remotely by a Remote Driver. Maximum speed 30 km/h.	X	
UC5.4-030	Handover for push movement in shunting	Remote operation in shunting. A maximum shunting speed of 30 km/h is assumed.	X	

4.5 CHAPTER 9: PEDESTRIAN DRIVING

Chapter 9 describes operations for a remote driver near the train.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-031	Initiate handover by pedestrian remote driver	A pedestrian driver claims responsibility for a train. The remote driver who was in control grants the responsibility.	X	X
UC5.4-032	Initiate handover by pedestrian driver	A pedestrian driver claims responsibility for a train currently under responsibility of another pedestrian driver. The pedestrian driver who was in control grants the responsibility to the other.	X	X
UC5.4-033	Move the train locally by pedestrian driver	The pedestrian driver moves the train in creeping speed and controls the traction power.	X	X

4.6 CHAPTER 10: TRANSVERSE TOPICS

Chapter 10 contains operations that are present in any typical condition – driver vitality check, sounding the horn.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-034	Warn its environment by the starting train	A Remote Driver monitoring a train claims responsibility for the train. The train, that was driving autonomously, creates the conditions for the take-over. The take-over takes place.	X	X
UC5.4-035	Board a train by driver.	An on-board driver wants to board on or off a train. He/she locks train motion by pushing the button on the doors boarding box at his/her side. Once finished with boarding. He/she releases the train motion by pushing again the button on the boarding box at his/her side. Several start conditions are gathered: train ready to board, already booked for motion.	X	X

4.7 CHAPTER 11: ADDRESSING DEGRADED MODES OF THE AUTONOMOUS TRAIN

Chapter 11 contains use cases in the event of a failure in the automation system.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-036	Take responsibility of a GoA3 train with degraded ATO by remote driver	The train is originally in GoA3. The ATO is in fault and the Remote Driver takes responsibility for the train (*1)		X
UC5.4-037	Take responsibility of a GoA4 train in degraded ATO situation	The train is originally GoA4. The ATO is in fault and the Remote Driver takes the train responsibility (*1). This use case provides remote train control operation by a driver in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself.		X
UC5.4-038	Take responsibility after some degraded PER in GoA4 mode by remote control driver	This use case describes when the Remote Driver takes the responsibility of the train in the degraded ATO GoA3 condition. This use case provides remote train control operation by a driver in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself.		X
UC5.4-039	Take responsibility after some degraded PERception in GoA4 mode by remote control driver	The Perception PER for GoA4 operation is in fault and the Remote Driver takes the train responsibility		X
UC5.4-040	Take responsibility after some degraded APM in GoA4 mode by remote control driver	The Automatic Processing Module (APM) is in fault and the Remote Driver takes the train responsibility		X

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-041	Take responsibility in degraded ETCS by remote control driver	This use case provides remote train control operation by a driver in the control centre, with degraded on-board ETCS. The Remote Driver should be able to drive the train remotely as if on the train itself. Caution: this use-case foresees in step 6 the isolation of ETCS. This strongly degrades the safety of the trains motion. Current use-case is intended only as exceptional procedure e.g., to drive a stopped train to a rescue point and bring the complete system back to normal operations. Specific regulations should guarantee safety before step 6 is taken – see for instance step 4 and 5. See also R1 in Appendix 1, Refinements, p.157.		X
UC5.4-042	Drive remotely in case of wayside signalling system failure	This use case provides remote train control operation by a driver in the RSC. The Remote Driver should be able to drive the train remotely as if on the train itself.		X

4.8 CHAPTER 12: DEGRADED MODES SPECIFIC TO REMOTE CONTROL

Chapter 12 describes operations while some fault occurs in the process chains of the remote control itself.

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-043	Drive remotely with a poor visibility due to weather	The visibility provided to a Remote Driver is not as good as expected. This use case drafts a strategy to avoid hazardous motions, while providing availability.	X	X
UC5.4-044	Drive remotely with a poor up-link connection	The quality of connection between train and RSC does not allow an optimal transmission of video and sound to the Remote Driver.	X	X

Id	Name	Summary	Planned GoA1-2	GoA3-4 fall-back
UC5.4-045	Drive remotely and loose track sensors	This use case happens during remote train control operation by a driver in the control centre. At least one perception sensor (camera) doesn't work properly.	X	X
UC5.4-046	Drive remotely with a poor down-link connection	The quality of connection between train and RSC does not allow an optimal transmission of commands to the train. The use case does not address the fact that a command cannot be executed as such because the component executing it is defect. Analysis of degrade mode is another scope. This use case covers only delay in the flow of command and their execution.	X	X

4.9 OBSOLETE USE CASES

Since the first version of the document, following use cases have been deleted, merged or underwent changes so big that it seemed appropriate to discontinue them and replace them by a new requirement.

Id	Name	Summary
UC5.4-002	Obsolete: merged into UC5.4-047 in edition 04	Traceability
UC5.4-003	Obsolete: merged into UC5.4-047 in edition 04	Traceability
UC5.4-004	Obsolete: merged into UC5.4-047 in edition 04	Traceability
UC5.4-005	Obsolete: merged into UC5.4-047 in edition 04	Traceability
UC5.4-006	Obsolete: merged into UC5.4-047 in edition 04	Traceability

5 CONNECTION BETWEEN TRAIN AND REMOTE SUPERVISION CENTRE

This chapter defines the registration of a train at some remote supervision centre. See [SRDC TAURO] for foundation works. It does not deal with network registration. Network registration is considered a technical use case completed prior to the use cases in this chapter, typically seamlessly.

In this chapter, scenarios for registration or un-registration are clustered in 2 families:

- Train is at standstill: Those use cases typically support wake-up, saving energy between mission, detrainment.
- Train is moving: those use cases are all part of some handover of responsibility.

States associated to this chapter are explained in section 3.2, States.

In general, the idea behind this chapter is that a train potentially candidate for remote control registers seamlessly to its RSC(s). This way, when remote control is required,

- An autonomous train can call for help in the RSC via its lost alarm policy;
- If the RSC defines a RUS for each train, an on-board driver can call for help in the RSC without searching for the right point of contract;
- Somebody in the RSC can take control of the train comfortably: the search for the train is eased.

Some use-cases are provided where the train is specifically registered or unregistered by a user. Lasty, strictly autonomous trains (WP5.1) may not require this registration. They may also go through areas of low bandwidth in which the registration is given up. Registration can then resume, as soon as the train is on the network again, automatically or not.

5.1 REGISTER A TRAIN

The registration of a train at some remote supervision centre causes this train to be visible by the users of this remote supervision centre (Remote Driver, RU-Supervisor, …).

5.1.1 Register A Train At An Rsc

This use case is depicted on a sequence diagram by Figure 3.

Use case field	Description
ID	UC5.4-001
Use case name	Register a train at an RSC
Main actor	Remote Supervision Centre
Other actors	Serviceable train (Train), RU-Supervisor (RUS)
Use case summary	A train registers to one RSC. It ends being registered at all RSCs at which it shall be observed.
Applicability	Geographical: European level System level: RSC, Train

	Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	After the procedure, the train is available for Monitoring by the drivers managed by the RSC.	
Preconditions	The RSC is up and running. The train is in 'standby' or 'operative' but unregistered. The triggers of the scenario may be: • A successful network registration (network only!) by the train. Either the train or the RSC are notified about this success by the network layer. On this occasion, either one or the other takes the initiative of the RSC registration. Therefore, the scenario can be started by both RSC and train, i.e. the first message (TSC->Train) is optional. Optionally, this trigger could be part of the sequence taken by a train waking up by itself (UC5.1-001). • Motion: The train drives along the borders of RSCs along its mission – see use case UC5.4-007. Note: this is independent of who is responsible for the train - it may be fully autonomous or drive autonomously under monitoring or control of a driver. • A RUS or an on-board driver triggers this registration via his/her HMI, for instance in the context of a train wake-up, or some maintenance. In this case, the train is for instance addressed by its IP address.	
Termination outcome	**Successful outcomes**	After the procedure, the train is registered, i.e. available for Observing by the drivers managed by the RSC-Centre. The RSC is registered by the train - potentially among several.
	Unsuccessful outcomes	The train is not registered at the remote supervision centre. It has not registered the remote supervision centre.
Condition affecting termination outcome	**Outcome 2**	The general state of the train (level of operations, driver already in charge) will affect the services available for Remote Drivers.
Use case description	**Step 1.0** **(optional)**	RSC: On one of the triggers of the pre-conditions, RSC sends a 'RegistrationRequest" to the train. It contains the *Supervision Centre Information* .
	Step 1.1	Train: sends a 'RegistrationRequest' to RSC As a request to step 1.0 or due to an independent trigger, for instance the train approaching RSC's observing area. It contains the train's observation information.
	Step 2.0	RSC: receives Step 1.1 message.

		The request may be approved automatically or by some Railway undertaking supervisor. In any case, RSC can send 2 responses: RSC refuses. From now on, it views the train as 'unregistered'. It sends a RegistrationRefusal: Branch to Step 3.0 RSC agrees. It inserts the train in its list of registered (observable) trains and sends a RegistrationConfirmation: Branch to Step 3.1
	Step 3.0	[The train receives RSC's refusal] The train reports a RegistrationFailureAlarm to its driver, be it an on-board driver, a Remote Driver depending on another RSC, or the automation component of a purely autonomous train with an alarm. In case of a purely autonomous train, the alarm is forwarded to the Lost Alarm Policy of the train's already registered RSCs. The use case ends in a failure. Branch to postconditions.
	Step 3.1	[The train receives RSC's confirmation] The train considers itself registered. It registers RSC in the list of centres it reports to. Branch to postconditions.
Postcondition	The train runs at least in 'standby' or 'operative': this has not changed since scenario start (pre-conditions). The Remote Supervision Centre is up and running - it has not changed since scenario start (pre-conditions). On success, the train is 'registered' at the supervision centre: It counts RSC in its list of the Remote Supervision Centres it shall report to, and RSC counts the train in its list of registered trains. On failure, the train does not count RSC in its list of registered, and RSC does not count the train in its list of observable train. The driver (or the lost alarm policy's receiver) receives an alarm. He/she is free to take contact to create the conditions of success. Note that even with a refusal, the train does not stop. It may stop when reaching the limit of the control area of the RSC it reports to (lost alarm policy).	
Use case notes	[SRS X2Rail-4 v0.3.0] talks about battery protection, energy saving mode, service retention (Standby). I could not find the exact definition of those modes in v 0.2.1. Therefore, current document defines some levels of operations. These definitions intend to prepare merging with X2Rail-4.	

UC5.4-001 Register a train at an RSC

5.2 REGISTER AND UNREGISTER A MOVING TRAIN

Along its journey, a train may be under the responsibility of several Remote Drivers, themselves hosted by several RSCs. To this intend, they have to register or unregister along their motion.

5.2.1 Register A Moving Train At An Rsc

This use case is supposed to support handover while a train changes the area of responsibilities of RSCs.

Use case field	Description	
ID	UC5.4-007	
Use case name	Register a moving train at an RSC	
Main actor	Serviceable train (Train)	
Other actors	Remote Supervision Centremote supervision Centre (RSC), Driver (On-Board, Remote)	
Use case summary	In this use case, a train detects automatically that it approaches the border of some RSC's area of observation.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	After the procedure, the train is available for Monitoring by the drivers managed by the centre2.	
Preconditions	The train runs with following state: • Remote Supervision Centre (Centre2): Unregistered • Remote Supervision Centre (Centre1): registered • Level of operations: Operative • User registration: GoA4, with or without monitoring human, Controlling On-board Driver or Controlling Remote Driver in centre 1 The train relies on following information: - The RSCs it reports to. Centre1 is one of them. - The list of their neighbouring RSCs. Centre 2 is a neighbour of centre 1. - The RSCs that shall be responsible for the train on the mission path. Centre2 follows Centre1. The train approaches the area of observation of centre 2.	
Termination outcome	**Successful outcomes**	After the procedure, the train is registered at Centre1 and Centre2. The responsible of the train (GoA4, Driver) is unchanged.

	Unsuccessful outcomes	The train is not registered at centre 2. It issues an alarm for its driver in charge (GoA4: see lost alarm policy).
Condition affecting termination outcome	**Outcome 2**	Loss of network may lead to an abrupt termination without success. The train falls back in state 'Unregistered-Stand-Alone'. This case in not considered in the postconditions. See use case UC5.4-044 for the associated postconditions.
Use case description	**Step 1.0** **(optional)**	The train identifies Centre2 as a centre in which some Remote Driver may want to monitor or control it: • It may be because Centre2 is specified as responsible on the mission path (options) • It may be because Centre2 is a neighbour of currently responsible centre1 • It may be due to a combination of the 2 As this is only registration, the train does not need to be sure that a driver awaits it in the centre. Before entering the area of observation of centre2, the train sends to Centre2 a RegistrationRequest.
	Step 1.1	The same sequence happens as in use case UC5.4-001, "Register a train at some RSC".
	Step 2.0	The train is now registered at Centre2. Centre2 has communicated its neighbouring centres and their area of observation. In this list, it identifies the centres, in the area of observation of which it lies. It reiterates the use case for them.
Postcondition	The train runs with following state: • Level of operations: Operative • User registration: Same as in pre-conditions (has not changed during the use case). • RSC registration: The train is registered at Centre2 and at Centre2's neighbours if it lies in their area of observation. ○ Centre1: registered (as before) ○ Centre2: registered (new) ○ Centre2Neighbours: registered if the train lies in their area of observation, Unregistered otherwise	
Use case notes	Nothing prevents the system to perform the unregistering from Centre1 (UC5.4-008) Found no X2Rail-4 equivalent.	

UC5.4-007 Register a moving train at an RSC

5.2.2 Unregister A Moving Train From An Rsc

Use case field	Description	
ID	UC5.4-008	
Use case name	Unregister a moving Train from an RSC	
Main actor	RSC Centre1	
Other actors	Serviceable train (Train), RSC Centre2, Remote Driver RD	
Use case summary	A train exits the area of observation of some RSC. It unregisters.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	After the procedure, - the train is not present in the list of trains provided by Centre1 to its drivers, and - the Centre1 is not in the list of centres the train shall report to.	

Preconditions	Centre1 and Centre2 are up and running.
	The train runs with following state:
	• Level of operations: operative
	• RSC registration:
	  ○ Centre1: registered
	  ○ Centre2: registered
	• User registration (RD2): monitoring or controlling from Centre2	

Termination outcome	**Successful outcomes**	After the procedure, the train is unregistered at centre1. The responsible for the train has not changed (RD2).
	Unsuccessful outcomes	The train has stopped to retain its registration
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1.0**	The train is about to leave the area of observation of Centre1. It sends to Centre1 an UnregistrationMessage. • UnregistrationReason = LeavingAreaOfObservation • (no reconnection date) • If the Centre 1 receives the request, branch to Step 3.0
	Step 2.0	[Centre1 receives the train's UnregistrationMessage]

		Centre1's LostAlarmPolicy checks if another center should be named, that receives the train's lost alarms. If so, branch to Stepp 2.1 If the lost alarm policy of the train is already redirected to at least another RSC, Centre1 confirms the Unregistration by sending an UnregistrationMessage: • UnregistrationReason = LeavingAreaOfObservation Branch to Step 3.0
	Step 2.1	Center1's lost alarm policy sends to the train an UnregistrationRefusal Message. The train stops before the limit of Center1's observation area. The lost alarm policy informs its personal that a train is stopping to avoid going unleashed. Branch to unsuccessful outcome.
	Step 3.0	The train archives the confirmation and deletes Centre1 from the centres it reports to.
Postcondition	The train is still registered at centre 2. The train is not registered anymore at Centre 1. Centre1 is a neighbour of at least one of centres the train currently reports to. Therefore, the train continues to monitor the border of Centre1's area of observation. Should it cross it again (entry), it would register again. RD2 is still monitoring of controlling the train.	
Use case notes	Found no X2Rail-4 equivalent.	

UC5.4-008 Unregister a moving Train from an RSC

6 BRINGING A TRAIN TO OPERATIONS

This chapter addresses the typical use cases where a Remote Driver comes to monitor a train. He / she does not yet control the train, hence needs first to monitor it, then to take control.

6.1 LOGGING ON A STANDBY TRAIN

6.1.1 Log-In On A Registered Standby Train

Use case field	Description	
ID	UC5.4-009	
Use case name	Log-in on a registered standby train	
Main actor	Remote Driver RD	
Other actors	Serviceable train (Train), Remote Supervision Centre (RSC)	
Use case summary	RD logs on a train initially registered and in standby. The RD is granted a monitoring access: display of train state; no control.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	After completion of this scenario, RD is monitoring the train. Among others, he/she has the capability to request control of the train.	
Preconditions	The train runs in state: • RSC registration: registered • Level of operations: standby • User registration (RD): Observing.	
Termination outcome	**Successful outcomes**	RD is monitoring the train, e.g. he / she can request control of the train.
	Unsuccessful outcomes	RD has not been granted Monitoring status of the train.
Condition affecting termination outcome	**Outcome 2**	Loss of network may lead to an abrupt termination without success. The train falls back in state 'Unregistered-Stand-Alone'. This case in not taken into account in the postconditions. See use case UC5.4-044 for the associated postconditions.
Use case description	**Step 1**	RD chooses a train in the fleet he/she is allowed to manage (competency, geography). He / she adds this train to the list of trains he/she is Monitoring.
	Step 2.0	Automatically, the RSC issues a RemoteMonitoringRequest to the train.

	Step 3.0	[The train receives the message issued in 2.0] The train checks if the user is allowed to monitor the train. If not, got to step 4.0. If yes branch to Step 4.1
	Step 4.0	[The train rejects the RemoteMonitoringRequest] It issues a diagnosis to the RSC. The reasons may be RD's competency profile, his/her company (railway undertaking). The use case ends without success: the train state is unchanged. The view of the train in the RSC is unchanged. Branch to postconditions
	Step 4.1	[The train allows the RemoteMonitoringRequest] The train sends an acknowledgement to the RSC. The train counts the user in its list of Monitoring users. The remote user monitors the train Branch to postconditions
Postcondition	The train runs in state: • RSC registration: registered • Level of operations: standby On success, RD monitors the train. On failure, RD still observes the train.	
Use case notes	-	

UC5.4-009 Log-in on a registered standby train

6.1.2 Take Control Of A Monitored Standby Train

Use case field	Description
ID	UC5.4-010
Use case name	Take control of a monitored standby train
Main actor	Remote driver RD1
Other actors	Serviceable train (Train), driver RODR2 (remote or on-board)
Use case summary	The RD1 is monitoring a train. The RD1 requests its control. On success, the RD1 has gained control of the train.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles

Main goal	After completion of this scenario, RD1 has control of this standby train. Among others he/she can wake-up the train – switch it to operative.	
Preconditions	The train runs in state: • RSC registration: registered • Level of operations: standby RD1 is monitoring the train, not yet controlling it. RODR2 may be controlling it already.	
Termination outcome	**Successful outcomes**	RD1 controls this standby train.
	Unsuccessful outcomes	RD1 still supervises the train.
Condition affecting termination outcome	**Outcome 2**	Loss of network may lead to an abrupt termination without success. The train falls back in state 'Unregistered-Stand-Alone'. This case in not taken into account in the postconditions. See use case UC5.4-044 for the associated postconditions.
Use case description	**Step 1**	RD1 issues a RemoteControlRequest by pushing the button RSC-ClaimGrant. The RSC checks the validity of RD1's control request, and potentially associated speed restrictions: - RD1 is certified for the train, incl. Its protection and communication system - RD1 is certified for the for the line on which the train will circulate The RSC sends to the train a control request for RD1. It contains RD1's certification profile: - Train types, potential speed restriction - Areas, potential speed restriction
	Step 2.0	The train receives RD1's request for control. It checks its validity: - RD1 is already monitoring the train. - RD1 is certified for the train, incl. Its protection and communication system - RD1 is certified for the line on which the train will circulate If the train deems the request invalid, it refuses the control. It sends to RD1 a refusal with appropriate diagnosis. RD1 remains in Monitoring. The use cases ended with a failure. Branch to step postconditions.

	Step 3.0	The train checks whether some RODR2 is already controlling the train. If not, the train grants control to RD1: it sends a confirmation message. The use case ends successfully – branch to postcondition. If RODR2 is already controlling the train, the train proceeds to step 4.0
	Step 4.0	[RODR2 is already controlling the train] The train sends to the HMI of RODR2 a 'Control request Alarm'. This alarm may comprise both visual and sound signals, according to the HMI of RODR2. If - RODR2 refuses the request (graphical interface, RSC-ClaimGrant long push) or - Ignores the alarms for GrantTimeOut seconds, the train refuses to grant DR1 control. It sends to DR1 a refusal with appropriate diagnosis. DR1 remains monitoring. Note: as the driver currently in charge, RODR2 is always allowed to refuse a control request. RD1 and RD2 are free to take contact with other to create the conditions of success. The use case ends with a failure. Branch to postconditions. If RODR2 issues a RemoteControlAcknowledgement by 1. pushing the button RSC-ClaimGrant, 2. or acknowledging the alarm on its graphical interface (pedestrian drivers) The train proceeds to step 4.1
	Step 4.1	The train grants control to RD1. It demotes RODR2 to Monitoring.
Postcondition	The train runs in state: • RSC registration: registered • Level of operations: standby On success, RD1 is controlling the train. If RODR2 was controlling the train at the beginning, RODR2 is now monitoring it. On failure, RD1 is monitoring the train. If RODR2 was controlling the train at the beginning, it still controls it.	
Use case notes	See also use cases in chapter 7, Negotiate Mastership, p.81.	

UC5.4-010 Take control of a monitored standby train

6.2 BRING A STANDBY TRAIN TO OPERATIONS

Next use-cases assume a train already monitored. They permit to promote the train to operative (UC5.4-010 to 012), incl. ETCS Start of Mission Procedure (UC5.4-013)

6.2.1 Wake-Up Train By Remote Driver

Use case field	Description	
ID	UC5.4-011	
Use case name	Wake-up train by remote driver	
Main actor	Remote Driver	
Other actors	Serviceable train (Train)	
Use case summary	A Remote Driver RD, already controlling a standby train (UC5.4-010), commands that it becomes operative.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	A Remote Driver who has logged on a train 'sleeping' starts its component so that the train becomes 'operative'.	
Preconditions	The train is in state: • RSC registration: registered • Level of operations: standby • User registration (RD): controlled The driver of this use case is the one controlling the train at use case start.	
Termination outcome	**Successful outcomes**	The train is "Operative".
	Unsuccessful outcomes	a) The train remains in a state is in "Controlled Standy"
Condition affecting termination outcome	**Outcome 2**	Loss of network may lead to an abrupt termination without success. The train falls back in state 'Unregistered-Stand-Alone'. This case in not taken into account in the postconditions. See use case UC5.4-044 for the associated postconditions.
Use case description	**Step 1**	The Remote Driver initiates the train wake-up e.g., by Graphical User Interface.
	Step 2	Train: switch on and power up. The train management wakes-up its automation systems:

		Mandatory: - The train's video and sound sensors are booted and directed to the controlling user workplace. - TCMS is booted and emerges with parking brake on. - ETCS is in Stand By without active cabin defined. If available: - ATO is booted - Perception / APM are booted
	2.1	Switch on components that are part of the definition of 'Operative'
	2.1.1	(mandatory) Switch on main power supply
	2.1.2	(mandatory) Switch on TCMS (mandatory)
	2.1.3	(mandatory) Switch on ETCS
	2.1.4	(mandatory) Switch on train video and sound sensors for Remote Driver cabin
	2.2	Switch on components that may not be necessary to be in operative already
	2.2.1	(optional) Switch on air conditioning
	2.2.2	(optional) Switch on light in train
	2.2.3	(optional) Switch on passenger information system
	2.2.4	(optional) Raise pantograph
	2.2.x	...
	Step 3	The train management assesses the boot of its automation systems and forwards their reporting to the controlling user. If all mandatory components are booted successfully, the use case is a success. Otherwise, the system enters a degraded mode that defines by the services provided by each to remote control. The philosophy is that of maximal availability in case of failure. Ex: if ATO failed, Remote video remains available. If the traction chain fails, TCMS decides to limit its traction services. Accordingly, ATO decides it is not available either. All tests depend on the train model and its brake strategy. Therefore, they are given exemplarily.
	Step 3.1	(Exemplarily) Check door control
	Step 3.2	(Exemplarily) Check passenger information system

	Step 3.3	(Exemplarily) Carry out brake test
	Step 3.4	(Exemplarily) Check the Horn
	Step 3.5	(Exemplarily) Check other devices
	Step 3.x	Refer to [STEST TAURO] for a comprehensive list of possible self-tests by a train.
Postcondition	The train is in state: • RSC registration: registered • Level of operations: Operative • User registration: Controlled (Remote Driver) The train further grants control to its user. It shares periodically its observation information with its controlling user and all monitoring user. This means in operative mode, additionally to observation information: ○ Remote video and sound ○ TCMS states & alarms ○ ETCS HMI information incl. alarms ○ ATO / DAS information ○ Perception / APM states and alarms It accepts control requests from the user, according to its accreditation limitations – also movement requests. It enables ATO-Engage.	
Use case notes	-	

UC5.4-011 Wake-up train by remote driver

6.2.2 Switch On Vehicle And Prepare It By Remote Driver

Use case field	Description
ID	UC5.4-012
Use case name	Switch on vehicle and prepare it by remote driver
Main actor	Remote Driver (RD)
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Remote Supervision Centre (RSC), On-board Automation System (OAS)
Use case summary	Train wakes up (UC5.4-011), then, the driver prepares it.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	Train is ready to operate.
Preconditions	The train is in state: • RSC registration: registered

	• Level of operations: standby. See operational definitions: Train is stabled in the train mode 'sleeping' with only the radio communication for wake-up powered including timer, temperature supervision, battery capacity supervision, slide supervision and cold movement detection. • User registration (RD): Controlled (e.g. UC5.4-010 completed)	
Termination outcome	**Successful outcomes**	• Outcome 1: Train is ready for service
	Unsuccessful outcomes	• A driver must enter the train and take control of the train
Condition affecting termination outcome	**Outcome 2**	The train could not be waked up. On-board maintenance personal shall be sent to the train to repair it.
Use case description	**Step 1**	RUS: request RD to prepare a specific train (if train is not switched-on).
	Step 1.1	OAS: wake-up command coming from a predefined timestamp while stabling sequence (if preset time is due before RD wake up).
	Train Wake-up (see UC5.4-011)	
	Step 2	RD: Initiate wake-up command.
	Step 3	OAS: receive wake-up command via radio communication for wake-up and battery main switch.
	Step 4	OAS: switch on train and power up. See UC5.4-011: step 2.x
	Step 5	OAS: perform self-test of activated components as necessary and as possible. See UC5.4-011: step 3.x
	Preparation by driver	
	Step 6	RD: Check that the Steps 2 to 5 were successful. On success, proceed with step 7. On failure, branch to outcome 2.
	Step 7	OAS: provide train status and grant remote control.
	Step 8	RD: identify train orientation and remotely activate respective cabin.
	Step 9	OAS: inaugurate train according to remotely activated cabin and provide live video, audio, and status information to RD via RSC.
	Step 10	RD: confirm length of train consist.
	Step 11	Train: check head/tail lights (it the train's TCMS can perform this check). Or RD: check head/tail lights via trackside CCTV (if the train cannot perform this check by itself).
	Step 12	RD: trigger brake test and observe reaction.
	Step 13	OAS: apply brakes and provide brake feed-back.

	Step 14	RD: checks brake feed-back.
	Step 15.1	OAS: send an alarm to RD (if brake test failed). RD is responsible not to drive the train remotely.
	Step15.2	RD: recognise insufficient brake capability if brake test feed-back is deviating expected reaction. RD is responsible not to drive the train remotely.
	Step 16	RD: check train status report for failure messages.
	Step 17	RD: enter country ID, train data, driver ID and IM area code.
	Step 18	RD: check live video, audio, and status information to be consistent to location and orientation.
Postcondition	The train is ready to be operated.	
Use case notes	The various components of the train: auxiliary power supply, battery charger, HVAC, lighting, head/tail lights, traction control, brake control, door control, automatic train protection, automatic processing module, automatic driving module, remote control unit, data communication units, … are powered on according to the selected train mode. Hence, there is no need for individual control by the Remote Driver.	

UC5.4-012 Switch on vehicle and prepare it by remote driver

6.2.3 Perform ETCS Start Of Mission Procedure By Remote Driver

Apart from exceptional use-case UC5.4-041, remote driving without ETCS protection is prohibited. This use case describes the ETCS's Start of Mission, as operated by a Remote Driver.

Use case field	Description
ID	UC5.4-013
Use case name	Perform ETCS start of mission procedure by remote driver
Main actor	Remote Driver (RD)
Other actors	Serviceable train (Train), Trackside automation System (TAS), ETCS-OB DMI
Use case summary	This use case provides remote train control operation to a driver in the RSC. The driver performs an ETCS Start of Mission procedure. After this, the Remote Driver should be able to drive the train remotely as if on the train itself. It is assumed that everything is working properly.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	The main goal of this use case is to enable seamless train control by a Remote Driver, by preparing ETCS-OB for it.
Preconditions	The train runs in state: • RSC registration: Registered • Level of operations: Operative • Standstill

	The driver is controlling the train. Communication between the train and the control centre is working correctly. All internal tests have been performed and the train is ready to go.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver and ready to move under ETCS protection.
	Unsuccessful outcomes	The train cannot be remotely controlled under ETCS protection.
Condition affecting termination outcome	**Outcome 2**	Communication failure.
Use case description	**Step 1**	RD: initiates the ETCS start of mission procedure.
	Step 1.1	(remote) ETCS-OB: starts the SoM procedure. Shows in the remote ETCS-DMI the SoM dialogs.
	Step 1.3	RD: inserts the values in the remote ETCS DMI and when requested confirm them: Driver ID, Level ETCS, Train data
	Step 2.1	EVC transfers its mission information to ATO.
	Step 2.2	EVC transfers its train data to TCMS.
	Step 4.1	(optional) Train: asks TAS for a journey
	Step 4.2	(optional) TAS: delivers the train with a journey
	Step 5	End of UC
Postcondition	• The driver is controlling the train. • The train is at standstill. • ETCS protects the train's movements. • The driver may start driving the train manually (UC5.4-024) or may engage ATO if Steps 4.x have been performed.	
Use case notes	-	

UC5.4-013 Perform ETCS start of mission procedure by remote driver

6.3 LOGGING ON AN OPERATIVE TRAIN

Next two use-cases permit to reach monitor a train already operative (for instance having realized the equivalent of UC5.4-01 to 012 automatically or controlled by another user). Taking control of the train (UC5.4-022 p. 96) is then possible.

6.3.1 Log-In On An Operative Train By Remote Driver

Use case field	Description
ID	UC5.4-014
Use case name	Log-in on an operative train by remote driver
Main actor	Remote Driver RD1
Other actors	Serviceable train (Train), Remote Driver RD2
Use case summary	RD1, observing a train already in operations under the control of RD2, logs-in on this train. The ED1 ends up monitoring the train.

Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	RD1 ends with a monitoring access, e.g. pre-requisite for a handover.	
Preconditions	The train is in state: • RSC registration: registered • Level of operations: operative RD2 is in control of the train. RD1 is observing the train.	
Termination outcome	**Successful outcomes**	The train state is unchanged. RD2 still controls the train. RD1 monitors the train.
	Unsuccessful outcomes	RD1 is not monitoring the train.
Condition affecting termination outcome	**Outcome 2**	Loss of network may lead to an abrupt termination without success. The train falls back in state 'Unregistered-Stand-Alone'. This case in not taken into account in the postconditions. See use case UC5.4-044 for the associated postconditions.
Use case description	**Step 1**	RD1 chooses a train in the fleet he/she is allowed to manage (competency, geography). He / she adds this train to the list of trains he/she monitors. The RSC issues for the Remote Driver a RemoteMonitoringRequest to the train.
	Step 2	[The train receives the message issued in 1] The train checks if the user is allowed to monitor the train. If it agrees to the RemoteMonitoringRequest, jump to Step 4. If not, jump to step 3.
	Step 3	[The train rejects the RemoteMonitoringRequest] It issues a diagnosis to the remote supervision centre. The reasons may be the competency profile of the driver, his/her company (railway undertaking), the areas of certification of the driver not matching with its current position. The use case ends without success: - The train does not add RD1 to its list of monitoring drivers. RD1's workplace issues an alarm/error message to user 1, incl. due diagnosis. The train is taken off from its monitored train list. - RD2 still controls the train.

	Step 4	[The train allows the RemoteMonitoringRequest] The train sends its acknowledgement to the RSC. It adds user 1 in its list of monitoring users. User1 gets a confirmation. RD2 receives an alarm 'monitoring user added'.
Postcondition	The train is in state: • RSC registration: registered • Level of operations: Operative RD2 is in control of the train. On success, RD1 is observing the train. On Failure, RD1 is still monitoring the train.	
Use case notes	-	

UC5.4-014 Log-in on an operative train by remote driver

6.4 DEMOTING AN OPERATIVE TRAIN, LOGGING OFF

In use cases UC5.4-015 and -016, a driver goes from monitoring to uninvolved. In this context, the train may be demoted back to standby (UC5.4-047) first.

6.4.1 Demote A Train From Operative To Standby By Remote Driver

This use-case mirrors UC5.4-011's awakening.

Use case field	Description
ID	UC5.4-047 { Created during review }
Use case name	Demote a train from operative to standby by remote driver
Main actor	Serviceable train (Train)
Other actors	Remote Supervision Centre (RSC), optional Remote Driver RD
Use case summary	On user request, the train switches from Operative to Stand-by.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	At the end of this use-case, the train is standby: it has restrained its services in order to save energy. It offers services to get back to operative.
Preconditions	The train runs with following state: • RSC Registration (Centre1): Registered • Level of operations: Operative • User registration (RD): Controlling • ETCS Mission is ended

Termination outcome	**Successful outcomes**	After the procedure, the train is in standby. According to TUM-10.1, -10.2, 7.3.3.1.2 in [SRS X2Rail-4 v0.3.0], the train can be waken-up again at any time by RU (see also UC5.4-009 to –011).
	Unsuccessful outcomes	1) The train remains operative 2) The train is no longer operative but a key component refused to switch off.
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1.0**	RD: request the train to switch to standby, with or without a wake-up date (see [SRS X2Rail-4 v0.3.0], §7.3.3.1.3.)
	Step 2.0	Train: checks whether the conditions to switch to standby are fulfilled: 1. Train is at standstill, 2. Parking brakes are applied 3. ETCS mission is ended If the conditions are not fulfilled, step to 2.1, step to 3.x else
	Step 2.1	The train refuses the request. It issues an appropriate diagnosis to RD. Branch to unsuccessful outcome 1. (RD may re-enter the use-case after he/she has created the conditions of success).
	3.x Decentral Switch off	In this switch-off wave, components are switched off, that may be switched-off by TCMS while it switches off itself (Step 4.3). They are not formally necessary for the train to be operative (see definition, some degraded operative is allowed). Switching those components off in advance permits to maintain the key components below up and running during the switch-off – maximum availability for the user/driver. The use-case does not decide how the sequencing is done, or forces to this sequencing. It only illustrates which that some components can be switched off before the components key for RTO. All 4.x steps are performed by the train.
	Step 3.1	Switch off components that may not be necessary to be in operative already
	Step 3.2	(optional) Switch off air conditioning
	Step 3.3	(optional) Switch off light in train

	Step 3.4	(optional) Switch off passenger information system
	Step 3.5	(optional) Lower pantograph
	Step 3.n	...
	4.x Switch off TRO key components	Following components are key to remote operations. To provide maximum availability to the driver (also diagnosis during switch-off), they are switched-off in a last wave. All steps are mandatory. All 4.x steps are performed by the train.
	Step 4.1	(mandatory) Switch off train video and sound sensors for Remote Driver cabin
	Step 4.2	(mandatory) Switch off ETCS
	Step 4.3	(mandatory) Switch off TCMS (mandatory)
	Step 4.4	Train: Check that the shutdowns 4.1 to 4.3 succeeded. If one or more was unsuccessful, • Train provides RD with an appropriate diagnosis • Branch to step 5.5 If all were successful, proceed to Step 4.4
	Step 4.5	RD: Consider next step. a) If RD decides to remain in control, branch to unsuccessful outcome 2 RD may command the train to operative again (UC5.4-011) to create the conditions of success. b) Force switch to standby Branch to Step 5.0
	Step 5.0	(mandatory) Switch off main power supply According to [SRS X2Rail-4 v0.3.0], only consumers directly connected to the battery are supplies. See definition
Postcondition	The train runs with following state: • RSC registration: registered • Level of operations: standby • User registration (RD): Controlling	
Use case notes	The user may now quit train control (UC5.4-015). After the procedure, the train is in standby. According to TUM-10.1, TUM-10.2, §7.3.3.1.2, TCMS-8.1 in [SRS X2Rail-4 v0.3.0], the train can be waken-up again at any time by RU (see also UC5.4-009 to –011).	

6.4.2 Demote A Remote Driver From Controlling To Monitoring

Use case field	Description	
ID	UC5.4-015	
Use case name	Demote a remote driver from Controlling to Monitoring	
Main actor	Remote Driver RD1	
Other actors	Serviceable train (Train), optional Remote Driver RD2	
Use case summary	RD1 is Controlling his/her train. He/she wants to get back to Monitoring.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	RD1 ends Monitoring the train.	
Preconditions	The train is in state: • RSC registration: registered • Level of operations: Operative • User registration: RD1 is Controlling the train. • Optional: RD2 may be Monitoring the train. • HMI: no driver control handover dialog is running	
Termination outcome	**Successful outcomes**	RD1 is Monitoring the train, now in monitored GoA4. RD2 is Monitoring the train – this state remains unchanged along the use-case.
	Unsuccessful outcomes	RD1 is still Controlling the train or The train has stopped or RD2 is Monitoring the train – this state remains unchanged along the use-case.
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1**	RD2: sends the train a RemoteControlDemoteRequest by a long push on the RSC-ClaimGrant button.
	Step 2	Train: receives the message issued in Step 1. Train checks if the user is allowed to start Monitoring the train: 1. ETCS is in full supervision 2. PER and APM are ready or up working

		3. ATO is ready or working If so, jump to step 4. If not, jump to step 3.
	Step 3	[The train refuses the RemoteControlDemoteRequest] It issues an alarm to RD1. The use case ends with a failure.
	Step 4	[The train allows the RemoteControlDemoteRequest] In addition to TCMS already running (by definition of operative), the train starts ATO and all components of autonomous driving if not yet started (PER and APM). The train (ATO) targets the autonomous max. speed if lower than current speed, so that after the transition, speed monitoring does not implement Emergency Brake Intervention. If any of those steps fails, jump to step 5. Jump to step 6 otherwise.
	Step 5	[The train refuses the RemoteControlDemoteRequest] The train issues an alarm to RD1. The train may have stopped (failure to reduce speed). The use case ends with a failure. RD1 remains in control of the train. Branch to postcondition.
	Step 6	The train demotes RD1 to Monitoring. The use case is a success.
Postcondition	The train is in state: • RSC registration: registered • Level of operations: operative RD2 is Monitoring the train – this state remains unchanged along the use-case. On success, RD1 is Monitoring the train, now in monitored GoA4. On Failure, RD1 is still Controlling the train. The train may have stopped. RD1 can take any measures to generate the conditions of success.	
Use case notes	Created while writing use cases. No traceability to X2Rail-4, TAURO.	

UC5.4-015 Demote a remote driver from controlling to monitoring

6.4.3 Stop Monitoring A Train By A Remote Driver

Use case field	Description

ID	UC5.4-016	
Use case name	Stop monitoring a train by a remote driver	
Main actor	Remote Driver RD1	
Other actors	Serviceable train (Train), optionally Remote Driver RD2, Remoter Supervision Centre (RSC), RSC's lost alarm policy.	
Use case summary	RD1 is Monitoring his/her train. He/she wants to stop this Monitoring.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	RD1 ends observing the train.	
Preconditions	The train is in state: • RSC registration: registered • Level of operations: Operative • User registration: RD1 is Monitoring the train. • User registration: RD2 may be Monitoring the train. • HMI: no driver control handover dialog is running	
Termination outcome	**Successful outcomes**	RD1 is no longer Monitoring the train. RD2 is Monitoring the train – this state remains unchanged along the use-case.
	Unsuccessful outcomes	RD1 is still Monitoring the train
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1**	RD1: sends the train a RemoteControlDemoteRequest by a long push on the RSC-ClaimGrant button.
	Step 2	Train: receives the message issued in Step 1 The train checks if RD1 is allowed to quit Monitoring the train. While monitoring, the driver has no duty, e.g. towards safety, for the train. So unlike for demoting controlling to monitoring, the 'allowance' meant here is not safety relevant. But if the only one monitoring driver of a train demotes to observing or uninvolved (full autonomy), the lost alarm policy of the train starts receiving the train's alarms. For availability reasons, the lost alarm policy may require that at least a RUS is named as addressee of the alarms.

		If allowed, jump to step 4, step 3 otherwise
	Step 3	[The train refuses the RemoteControlDemoteRequest] It issues an alarm to RD1 with appropriate diagnosis. The use case ends with a failure. Jump to postconditions.
	Step 4	[The train allows the RemoteControlDemoteRequest] The train sends a DemotingMonitoringDriverNotificaiton to other drivers Monitoring the train or to the lost alarm policy.
	Step 5	The train demotes RD1 to Observing
Postcondition	The train is in state: • RSC registration: registered • Level of operations: operative RD2 is Monitoring the train – this state remains unchanged along the use-case. On success, RD1is now Observing the train, now in monitored GoA4. On failure, RD1 is still Monitoring the train – unchanged still start – with an appropriated diagnosis of the failure reasons. RD1 is free to generate the conditions of success, e.g. he/she requests that a RUS is named addressee of the alarms.	
Use case notes	Created while writing use cases. No traceability to X2Rail-4, TAURO.	

UC5.4-016 Stop monitoring a train by a remote driver

7 NEGOTIATE MASTERSHIP

This chapter deals with mastership- negotiation between on-board and Remote Driver in a RSC.

The assumption taken is a post-autonomy RSC. Use-cases in which a driver is needed are likely to be related to degraded system – malfunction of the obstacle avoidance of a train, defect level crossing, particularly dangerous pedestrian hotspot with defect obstacle recognition...

In this context, drivers negotiating mastership may happen:

1. From on-board to remote drivers
2. From remote driver to other remote drives
3. From remote driver from/to full autonomy

The hand-over use cases between Remote Driver and AT (GoA34 train) should be identical or at least resemble as much as possible the corresponding use cases for hand-over between OB (i.e. local) driver and AT.

For 2. and 3. the current constraint that a driver boards the train before the handover has vanished. For 3., a driver may be called to inspect a still moving train (alarm). Therefore, in-motions handovers have been considered.

While ATO is a strong assumption in a post-autonomy world, remote control shall be available for degraded situations, in which ATO is not available anymore. Therefore use-cases have been introduced for both ATO-supported and manual use cases (high availability principle).

For mastership- negotiation with pedestrian drivers, please refer to chapter 2, Pedestrian Driver, p.119.

For all use cases in this chapter, the train runs in state:

- Remote Supervision Centre: registered
- Level of operations: operative

Several drivers may be implied, unless the use case involves a train in GoA4 (controlling it, monitoring it, or release it completely to a level autonomy without defined Remote Driver). These drivers may be monitoring or controlling.

7.1 COMMON SEQUENCES

7.1.1 Confirm Remote Driver Vitality By Remote Driver

For the train's safety, it is essential to check the driver vitality regularly to avoid dangerous situations due to inattention of driver or his unavailability caused by whatever reason. It is therefore, crucial to use a similar method for checking the vitality of Remote Drivers. This use case details the Remote Driver vitality check during remote train control.

The Remote Driver is required to confirm its vitality at regular intervals using the vitality operating element. He is alerted to the necessity of this action by an audible and visual signal. In the case of another action, e.g. change in driving speed, this action is also taken as a confirmation of the Remote Driver's vitality.

Use case field	Description	
ID	UC5.4-017	
Use case name	Confirm remote driver vitality by remote driver	
Main actor	Remote Driver RD	
Other actors	Serviceable train (Train), Railway Undertaking Supervisor (RUS) Infrastructure Incident manager (IIM) HMI component: Remote train operation HMI	
Use case summary	This use case details the periodic checking of Remote Driver vitality during remote train control to check attention to the screen.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The primary objective of this use case is to outline the procedure for regularly assessing the alertness of the Remote Driver.	
Preconditions	The train is operative. RD is controlling the train. Train is moving or is standing.	
Termination outcome	**Successful outcomes**	The system successfully checks that Remote Driver uses the vitality device periodically.
	Unsuccessful outcomes	The system did not successfully receive vitality confirmation (check) from Remote Driver.
Condition affecting termination outcome	**Outcome 2**	Communication failure between the vitality device and the train. Unfocused/absent Remote Driver
Use case description	**Step 1**	RD: drives the train.
	Step 2	Train. After [X] seconds since the last use of the vitality device, Train visually and audibly alerts RD to confirm his/her vitality.
	Step 3	Train: Has RD confirmed his/her vitality? If yes inform the system and continue with Step 1. If no, proceed to step 4.
	Step 4	[After [Y] seconds since the beginning of alerting by the system (step2), without confirmation by RD] Train: stop and inform RUS and IIM.
	Step 5	Terminate use case.
Postcondition	The train is operative. RD controls it. On Success, • the system confirmed that Remote Driver is able to drive the train. • RD continues to drive On Failure	

	• the train has stopped • IIM and RUS are informed • IIM, RUS and RD try to engage contact to make sure RD is still capable to fulfil its mission. A procedure may be engaged to aid RD (health) and/or relieve him/her.
Use case notes	UC is mentioned to be performed periodically during whole operation of the train by Remote Driver, as soon as he/she is controlling a train. Related to [SRS X2Rail-4 v0.3.0], chapter 13.12.1 Remote Driving. The vitality confirmation is supposed to be performed by means of a button/pedal push. The current solution, however, does not exclude some eye tracking if confirmed by some Human Factor Analysis.

UC5.4-017 Confirm remote driver vitality by remote driver

7.2 HANDOVER WHILE DRIVING AT TRACTION CHAIN LEVEL

7.2.1 Initiate Handover From On-Board Driver By The Remote Driver, No ATO

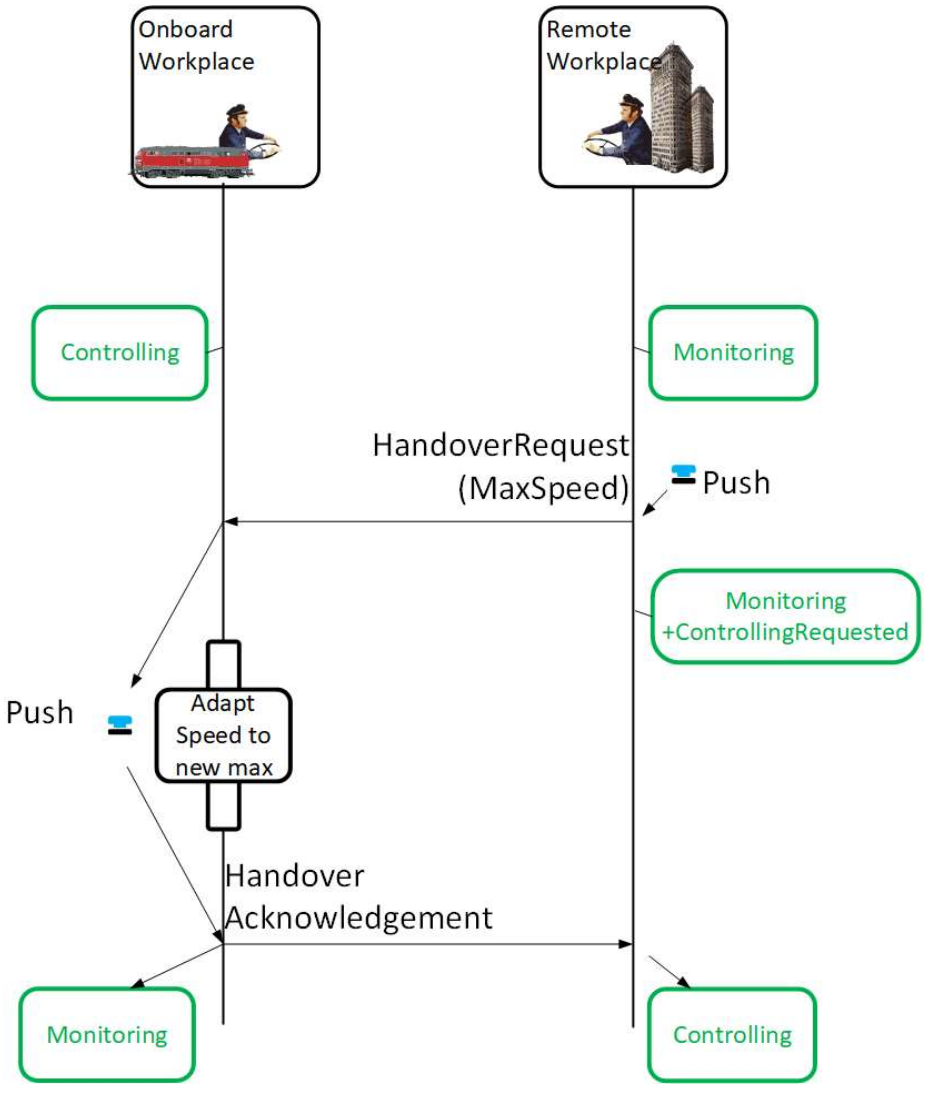

Figure 12: Monitoring driver requests handover, train driven at traction & braking chain level.

Use case field	Description	
ID	UC5.4-018	
Use case name	Initiate handover from on-board driver by the remote driver, no ATO	
Main actor	Remote Driver RD	
Other actors	Serviceable train (Train), On-board driver ODR	
Use case summary	RSR, monitoring a train, claims responsibility for this train. ODR, who was driving at traction chain level, grants the responsibility.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	At the end of the use case, RD drivers the train while the ODR monitors it.	
Preconditions	The ODR drives his/her train at traction/braking chain level. RD is already monitoring the train. The 2 drivers are linked via a voice channel.	
Termination outcome	**Successful outcomes**	RD is controlling the train. ODR is monitoring the train. Later on, he/she may resume his/her Monitoring.
	Unsuccessful outcomes	ODR is still controlling the train, although he/she had confirmed; RD is still monitoring the train
Condition affecting termination outcome	**Outcome 2**	ODR refuses or ignores the handover request. The handover does not take place.
Use case description	**Step 1**	RD issues a RemoteControlRequest by pushing his/her button RSC-ClaimGrant. The workplace computes a maximum speed V_Max_Driver function of its accreditation profile. It sends a HandoverRequest (V_MAX_Driver).
	Step 2	The train receives the claim from the RSC. It enhances V_Max_Driver with additional information it relies on visibility, video latency and quality of RemoteDriverWorkplace. This results in V_MAX_AFTERHANDOVER
	Step 3.1	An alarm is issued in the cabin of ODR (bell, lamp, DMI indication, ..) that means 'request to take-over by monitoring driver'.

		RD gets a message that the controlling driver is notified and, if so, that the train is driving too fast. ODR driver may decide: 1. ODR refuses (long push of RSC-ClaimGrant) or ignores the claim (timeout). Branch to 3.1.1 2. [Current speed > V_MAX_AFTERHANDOVER] a. ODR slows-down Branch to 3.1.2 b. ODR confirms handover with a Push on RSC-ClaimGrant Branch to 3.1.3 3. [Current speed <= V_MAX_AFTERHANDOVER] ODR confirms handover, the train driving under V_MAX_AFTERHANDOVER] Branch to 3.1.4
	Step 3.1.1	[ODR refuses or ignores the claim.] RD gets from its workplace an alarm 'HandOverRequest IgnoredOrRejected'. The use case finishes as Outcome2. Branch to postconditions. Note: The drivers may discuss their reasons on the voice channel. After this, the use case may be re-entered.
	Step 3.1.2	[Current speed > V_MAX_AFTERHANDOVER], [ODR slows-down.] ODR slows-down to V_New. ODR then: issues no answer to the RemoteControlRequest or issues a RemoteControlRefusal (long push to RSC-ClaimGrant), Independently of V_New. Branch to back to 3.1.1 [V_New <= V_MAX_AFTERHANDOVER] He/she issues a RemoteControlAcknowledgement with a Push on RSC-ClaimGrant. Branch to 3.1.4 [V_New > V_MAX_AFTERHANDOVER] The driver issues a RemoteControlAcknowledgement with a Push on RSC-ClaimGrant Branch to 3.1.3

	Step 3.1.3	[Current Speed > V_MAX_AFTERHANDOVER], [The on-board driver has confirmed the handover] The train implements a Service Braking Intervention. As soon as V_New < V_MAX_AFTERHANDOVER, Branch to 3.1.4
	Step 3.1.4	[Current speed <= V_MAX_AFTERHANDOVER], [The on-board driver has confirmed the handover] The handover takes place. Branch to postconditions.
Postcondition	See common conditions at chapter introduction. On success, • RD is now controlling the train. • ODR is now monitoring the train. On Outcome2 or on failure, • ODR is still controlling the train. • RD is still monitoring the train. The drivers may discuss their reasons on the voice channel. Once they have created the conditions for success, the use case may be re-entered	
Use case notes	Other take-over conditions may be defined, other than speed. For instance, if the responsible driver is already braking toward a reduction of max speed, and close to the breaking curve, then the driver in charge may be given the opportunity to finish its manoeuvre.	

UC5.4-018 Initiate handover from on-board driver by the remote driver, no ATO

7.2.2 Initiate Handover To Remote Driver By On-Board Driver, No ATO

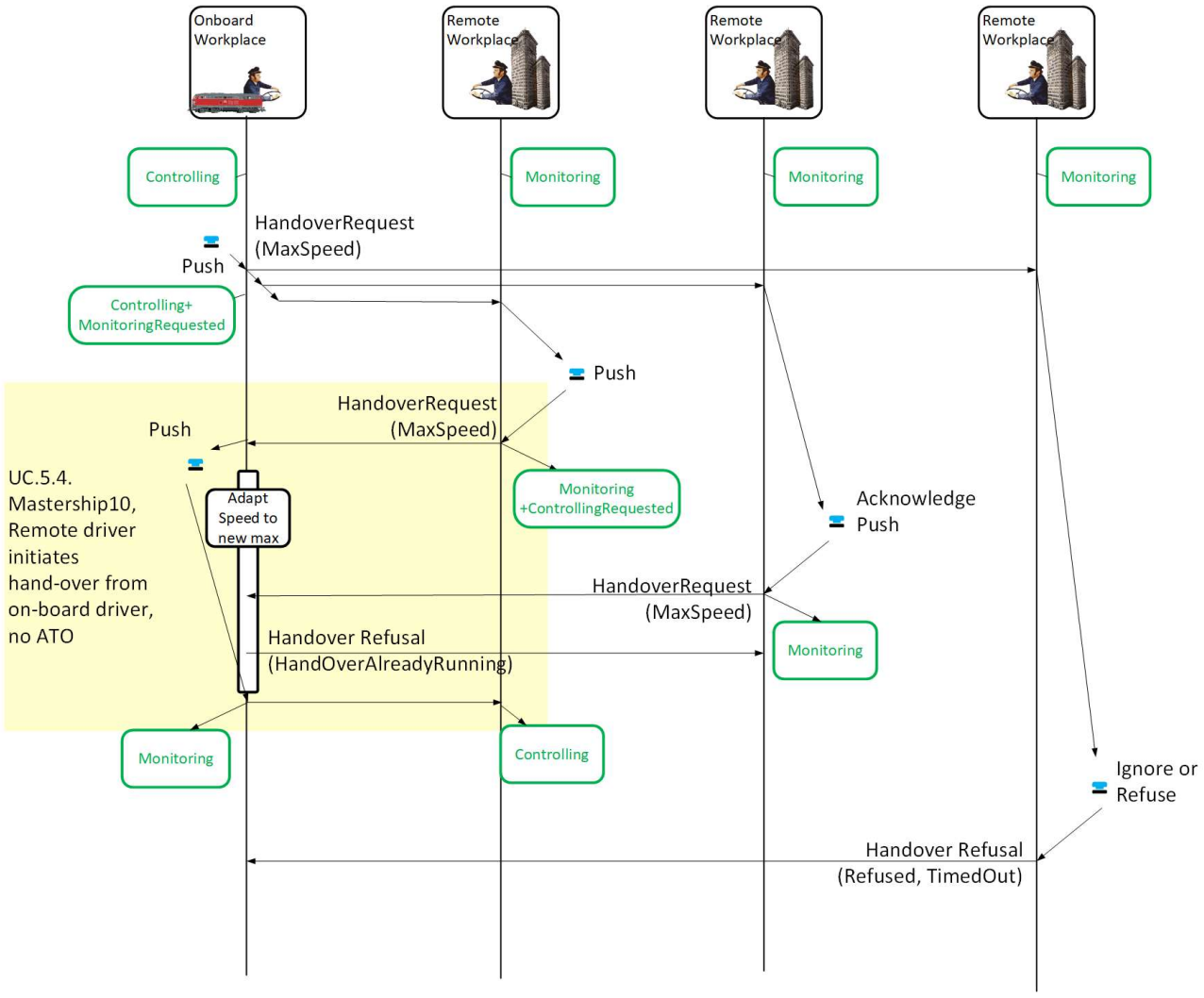

Figure 13:, Controlling driver requests handover

Use case field	Description
ID	UC5.4-019
Use case name	Initiate handover to Remote Driver by On-board driver, no ATO
Main actor	On-board train driver (ODR)
Other actors	Remote Driver (RD), Serviceable train (Train) HMI: Remote Supervision CentreSC: TS.Button.RSC-ClaimGrant , Train: OB.Button.RSC-ClaimGrant
Use case summary	An on-board driver, controlling train, asks for handover to a remote driver already monitoring the train. The remote driver, takes the responsibility. At the end of the use case, the remote driver responds for the train while the on-board driver monitors it.
Applicability	Geographical: European level

	System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	An on-board driver hands the train over to a remote driver while preparing to leave the train (end of his/her day). A full-competency-profile remote driver assists an on-board driver, for instance a GoA3 attendant.	
Preconditions	ODR is controlling the train. He/she drives his/her train at traction/braking chain level. RD is already monitoring the train. The 2 drivers are linked via a voice channel.	
Termination outcome	**Successful outcomes**	RD is controlling the train. ODR is monitoring the train.
	Unsuccessful outcomes	ODR is still controlling. RD still monitoring.
Condition affecting termination outcome	**Outcome 2**	Initial train speed, competence profile of RD.
Use case description	**Step 1**	ODR issues a HandOverRequest by pushing RSC-ClaimGrant.
	Step 2	The RSC receives the claim from the train. The RSC dispatches the request to all Remote Drivers monitoring the train at that moment. An alarm-bell rings at the workplaces of the Remote Drivers monitoring the train. On their DMI, a message appears even if they are monitoring another train, or several trains, at this time. This message enables taking voice contact with all drivers currently monitoring the train (controlling if any, monitoring). This message requests each driver to confirm or deny taking over. If at least one remote driver RD confirms, jump to step 3.0. Jump to step 4 otherwise.
	Step 3.0	[RD confirms the requests] From that point on, use case UC5.4-018, “Remote Driver initiates handover from on-board driver, no ATO” is executed, starting with step 2. For each further driver confirming the request, Branch to 3.1. Branch to 4 for the remaining drivers.

	Step 3.1	[For each Remote Driver that confirms the request after RD in Step 3.0] The driver answers with a handover request (maxspeed), as if UC5.4. Mastership-10 was starting. The initially controlling driver, however, answers with a Handover Refusal (RefusalReason). RefusalReason may be: 1) HandoverAlreadyRunning 2) Driver Monitoring (no handover possible any more) Note: this answering maybe taken over automatically by the train. Branch to Step 4.
	Step 4	[For each Remote Driver that refuses or ignores the request] His/her workplace sends to the train a handover Refusal with the reason for the refusal (refused, timeout). Jump to postcondition.
Postcondition	See common conditions at chapter introduction. On success, • RD is now Controlling the train. • ODR is now Monitoring the train. • Further remote drivers now are Monitoring the train. On failure, • ODR is still controlling the train. • RD is still monitoring the train. The drivers may discuss their reasons on the voice channel. Once they have created the conditions for success, the use case may be re-entered.	
Use case notes	This use-case may be useful on a line without autonomy, and with a depot difficult to reach. Drivers are given the possibility to board/leave the train at the last station. To avoid losing time at the platform, the handover happens after the first stop/before the last stop. The moment the driver wants to start preparing himself to leave the train is decided by the on-board driver.	

UC5.4-019 Initiate handover to Remote Driver by On-board driver, no ATO

7.2.3 Initiate Handover From Another Remote Driver By Remote Driver, No ATO

This use case is similar to UC5.4-018, "Remote Driver initiates handover from on-board driver, no ATO". It should be read with associated Figure 12: Monitoring driver requests handover, train driven at traction & braking chain , p.83.

Use case field		Description
ID		UC5.4-020
Use case name		Initiate handover from another Remote Driver by Remote Driver, no ATO
Main actor		Remote Driver RD1, claims Mastership
Other actors		Remote Driver RD2, grants Mastership, Serviceable train (Train)
Use case summary		RD1 initially monitoring a train claims responsibility for the train. RD2, who was driving at traction chain level, grants the responsibility.
Applicability		Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal		At the end of the use case, the RD1 responds for the train while the RD2 monitors it.
Preconditions		RD2 drives his/her train at traction/braking chain level. RD1 is already monitoring the train. The 2 drivers are linked via a voice channel.
Termination outcome	**Successful outcomes**	RD2 is controlling the train. RD1 is monitoring the train. Later on, he/she may resume his/her Monitoring.
	Unsuccessful outcomes	RD2 still controlling the train, although he/she had confirmed; RD1 is still monitoring the train
Condition affecting termination outcome	**Outcome 2**	RD2 refuses or ignores the handover request. The handover does not take place.
Use case description	**Step 1**	RD1 issues a RemoteControlRequest by pushing his/her button RSC-ClaimGrant. The workplace computes a maximum speed V_Max_Driver function of its accreditation profile. It sends a HandoverRequest (MaxSpeed).
	Step 2	The train receives the claim from the RSC. It enhances MaxSpeed V_Max_Driver with additional information it relies on: visibility, video latency of RemoteDriverWorkplace.

		This results in V_MAX_AFTERHANDOVER.
	Step 3.1	An alarm is issued at RD2's workplace (bell, lamp, DMI indication) that means 'request to take-over by monitoring driver'. RD1 gets a message that the RD2 is notified and, if so, that the train is driving too fast. RD2 may decide: 1. RD2 refuses (long push of RSC-ClaimGrant) or ignores the claim (timeout). Branch to 3.1.1 2. [Current speed > V_MAX_AFTERHANDOVER] a. RD2 slows-down Branch to 3.1.2 b. RD2 confirms handover with a Push on RSC-ClaimGrant Branch to 3.1.3 3. [Current speed <= V_MAX_AFTERHANDOVER] RD2 confirms handover Branch to 3.1.4
	Step 3.1.1	[RD2 refuses or ignores the claim.] RD1 gets from its workplace an alarm 'HandOverRequest IgnoredOrRejected'. The use case finishes as Outcome2. Branch to postconditions. Note: The drivers may discuss their reasons on the voice channel. After this, the use case may be re-entered.
	Step 3.1.2	[Current speed > V_MAX_AFTERHANDOVER], [RD2 slows-down.] RD2 slows-down to V_New. Then: • RD2 issues no answer to the RemoteControlRequest or issues a RemoteControlRefusal (long push to RSC-ClaimGrant), Independently of V_New. Branch to back to 3.1.1 • [V_New <= V_MAX_AFTERHANDOVER] RD2 issues a RemoteControlAcknowledgement with a Push on RSC-ClaimGrant. Branch to 3.1.4

		• [V_New > V_MAX_AFTERHANDOVER] RD2 issues a RemoteControlAcknowledgement with a Push on RSC-ClaimGrant Branch to 3.1.3
	Step 3.1.3	[Current Speed > V_MAX_AFTERHANDOVER], [RD2 has confirmed handover] The train implements a Service Braking Intervention. As soon as V_New < V_MAX_AFTERHANDOVER, Branch to 3.1.4
	Step 3.1.4	[The on-board has confirmed handover, the train driving under V_MAX_AFTERHANDOVER] The handover takes place. Branch to postconditions.
Postcondition	See common conditions at chapter introduction. On success, • RD1 is now Controlling the train. • RD2 is now Monitoring the train. On failure, • RD1 is still controlling the train. • RD2 is still monitoring the train. The drivers may discuss their reasons on the voice channel. Once they have created the conditions for success, the use case may be re-entered.	
Use case notes	Other take-over conditions may be defined, other than speed. For instance, if the responsible driver is already braking toward a reduction of max speed, and close to the breaking curve, then the driver in charge may be given the opportunity to finish its manoeuvre.	

UC5.4-020 Initiate handover from another Remote Driver by Remote Driver, no ATO

7.3 HANDOVER WHILE DRIVING WITH ATO

7.3.1 Initiate Handover From Another Driver By Remote Driver, ATO Engaged

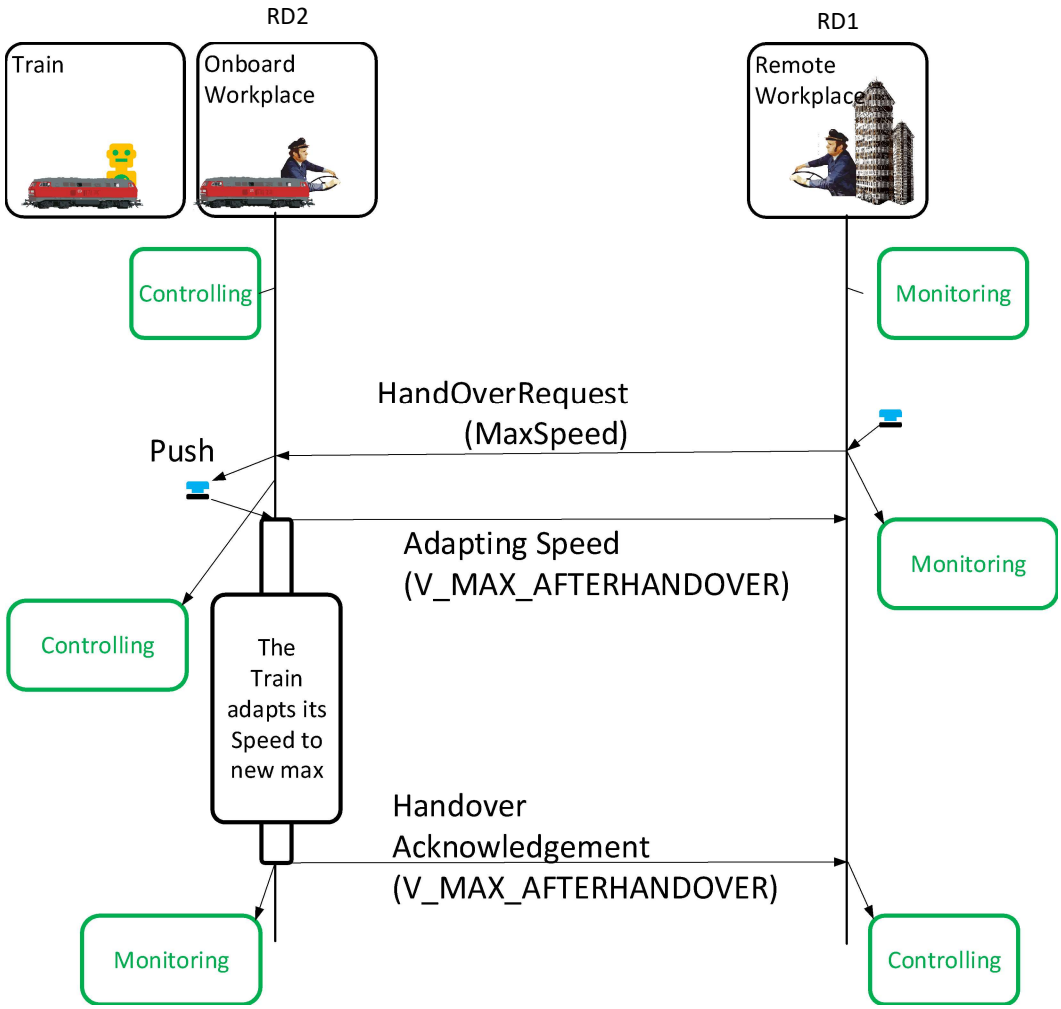

Figure 14: Monitoring driver requests handover, ATO engaged

Use case field	Description
ID	UC5.4-021
Use case name	Initiate handover from another driver by remote driver, ATO engaged
Main actor	Human: Remote Driver RD1, claims Mastership
Other actors	Human: Remote Driver RD2, grants Mastership, Serviceable train (Train)
Use case summary	A Remote Driver RD1 initially monitoring a train claims responsibility for the train. A second Remote Driver RD2, who was controlling the train with engaged ATO, grants the responsibility.

	At the end, the RD1 is controlling the train. The train has automatically adapted its speed to RD1's maximum driving speed.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	At the end of the use case, the RD1 responds for the train while the RD2 monitors it. For instance, a full-competency-profile Remote Driver assists a GoA3 attendant.	
Preconditions	RD2 drives his/her train with ATO engaged. RD1 is already monitoring the train (e.g. UC5.4-014). The two drivers may be linked via a voice channel.	
Termination outcome	**Successful outcomes**	RD2 is controlling the train. RD1 is monitoring the train. Later on, he/she may resume his/her Monitoring.
	Unsuccessful outcomes	RD2 still controlling the train, although he/she had confirmed; RD1 is still monitoring the train
Condition affecting termination outcome	**Outcome 2**	RD2 refuses or ignores the handover request. The handover does not take place.
Use case description	**Step 1**	RD1 issues a RemoteControlRequest by pushing his/her button RSC-ClaimGrant. The workplace computes a maximum speed V_Max_Driver function of its accreditation profile. It sends a HandoverRequest (MaxSpeed).
	Step 2	The train receives the claim from the remote supervision centre. It enhances MaxSpeed V_Max_Driver with additional information it relies on: visibility, video latency of RemoteDriverWorkplace. This results in V_MAX_AFTERHANDOVER.
	Step 3	An alarm is issued at RD2's workplace (bell, lamp, DMI indication) that means 'request to take-over by monitoring driver'. RD1 gets a message that the RD2 is notified and, if so, that the train is driving too fast. 2 further steps: 1. RD2 refuses (long push of RSC-ClaimGrant) or ignores the claim (timeout). Branch to step 4

		2. RD2 confirms handover with a Push on RSC-ClaimGrant Branch to step 5
	Step 4	[RD2 refuses or ignores the handover] RD2 sends a RemoteControlRefusal with appropriate diagnosis. The use case is finished. Branch to postconditions.
	Step 5.1	[RD2 confirms the handover] If [CurrentSpeed > V_MAX_AFTERHANDOVER], Branch to Step 5.2. Branch to 6 otherwise.
	Step 5.2	[CurrentSpeed > V_MAX_AFTERHANDOVER], [RD2 has confirmed the handover] ATO adapts its speed to V_MAX_AFTERHANDOVER. RD2 (its workplace) notifies RD1 with a message Adapting Speed (V_MAX_AFTERHANDOVER) that the handover is confirmed but the train speed is too high with the message 'Adapting speed'.
	Step 6	[CurrentSpeed <= V_MAX_AFTERHANDOVER], [RD2 has confirmed the handover] RD2 (its workplace) notifies RD1 that the handover is confirmed and successful with message Handover Acknowledgement (V_MAX_AFTERHANDOVER).
Postcondition	See common conditions at chapter introduction. On success, • RD1 is now Controlling the train. • RD2 is now Monitoring the train. On failure, • RD1 is still controlling the train. • RD2 is still monitoring the train. The drivers may discuss their reasons on the voice channel. Once they have created the conditions for success, the use case may be re-entered.	
Use case notes	-	

UC5.4-021 Initiate handover from another driver by remote driver, ATO engaged

7.4 TRANSITION FROM/TO AUTONOMOUS TRAIN

7.4.1 Initiate Handover From Autonomous Train By Remote Driver, ATO Engaged

Use case field	Description	
ID	UC5.4-022	
Use case name	Initiate handover from autonomous train by remote driver, ATO engaged	
Main actor	Remote Driver RD	
Other actors	Serviceable train (Train)	
Use case summary	RD monitoring a train claims responsibility for the train. The train, that was driving autonomously, creates the conditions for the take-over. The take-over takes place.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	A full-competency-profile remote driver RD takes control of an autonomous train.	
Preconditions	The train is driving autonomously. RD is already monitoring the train. No on-board driver is available in the train.	
Termination outcome	**Successful outcomes**	RD drives the train It relies on as much assistance as is available.
	Unsuccessful outcomes	The train still drives autonomously The train has stopped.
Condition affecting termination outcome	**Outcome 2**	Initial train speed Competence profile of RD.
Use case description	**Step 1**	RD issues a RemoteControlRequest with button RSC-ClaimGrant. The workplace computes a maximum speed V_Max_Driver function of its accreditation profile. It sends a HandoverRequest (MaxSpeed) to the train.
	Step 2	The train receives the request from the workplace. It enhances MaxSpeed V_Max_Driver with additional information it relies on: visibility, video latency of RemoteDriverWorkplace according to section 12.1.1, Video Latency, p.142. This results in V_MAX_AFTERHANDOVER

	Step 3.1.1	RD gets a message that the train is notified and, if so, that the train is driving too fast. The train decides: 1. [The train is driving under V_MAX_AFTERHANDOVER.] Branch to 3.1.3 2. [The train is driving over V_MAX_AFTERHANDOVER]: The train slows-down to meet the V_MAX_AFTERHANDOVER. Branch to 3.1.2
	Step 3.1.2	[The train is driving over V_MAX_AFTERHANDOVER] The train slows-down to some speed V_New lower than V_MAX_AFTERHANDOVER. Once this speed is reached, Branch to Step 3.1.3.
	Step 3.1.3	[The train is driving under V_MAX_AFTERHANDOVER.] The handover takes place. Branch to postconditions.
Postcondition	RD is now Controlling for the train, driving with ATO. The autonomous train functions, but for ATO, are now aiding RD. • The autonomous train's maximum speed is no more enforced by ETCS. • Obstacle detection is still up and running. It can stop the train at any time.	
Use case notes	-	

UC5.4-022 Initiate handover from autonomous train by remote driver, ATO engaged

7.4.2 Initiate Handover From Autonomous Train By Remote Driver, ATO Not Engaged

The Remote Driver engages ATO, and all systems of GoA4 are running, the message comes that he/she can engage GoA4: demote to Monitoring. This is reached by pushing ATO-engaged and RSC-claim grant with a long push.

Use case field	Description
ID	UC5.4-023
Use case name	Initiate handover from autonomous train by remote driver, ATO not engaged
Main actor	Remote Driver RD
Other actors	Serviceable train, Railway Undertaking Supervisor (RUS).
Use case summary	A remote driver supervising a train hands-over responsibility for the train. The train continues driving autonomously, after verifications that it is possible. The remote driver passes the train to the attention of supervisor.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles

Main goal	Verify the ability of the train to drive itself and handover its control to the on-board unit.	
Preconditions	RD driver the train. ATO is not engaged. The train is equipped in GoA4 components. Communication between remote control and train is fully functional.	
Termination outcome	**Successful outcomes**	Train continues mission in autonomous mode (GoA3/4). Supervisor is assigned to new GoA3/4 train in the area.
	Unsuccessful outcomes	The train was unable to take over control from Remote Driver. The train has stopped.
Condition affecting termination outcome	**Outcome 2**	Final train speed. Availability and vitality of GoA 3/4 components on the train. Availability and assigning of supervisor to the autonomous train.
Use case description	**Step 1**	RD performs a long push on button RSC-ClaimGrant . Workplace sends a HandoverRequest (RSC->Train).
	Step 2	The train receives the HandoverRequest (RSC->Train) from the RSC. It verifies following information at minimum: - Health of the necessary sensors (X2Rail-4: PERReadiness, APMReadiness). - Lost alarm policy guarantees that alarms needing acknowledgement, and that only a human can acknowledge, get distributed to a human, for instance the RU-Supervisor - ATO readiness ([SS-125], e.g. Availability of mission profile in train repository). - Available video quality and sensory distance capabilities for autonomous train operation (obstacle detection and reaction). This results in V_MAX_AFTERHANDOVER.

	Step 3	RD gets a message that the train is notified, able to drive autonomously, and if so, information for required speed reduction. Next steps depend on current train speed: A. [The train is driving under V_MAX_AFTERHANDOVER.] Branch to 3.1.0. B. [The train is driving over V_MAX_AFTERHANDOVER] B.1 RD lowers speed manually under V_MAX_AFTERHANDOVER. He/she then confirms with a new Long Push on RSC-ClaimGrant. Branch to 3.1.2 B.2 RD confirms with a Long Push, in spite of a current speed too high. Branch to 3.1.0.
	Step 3.1.0	[The train is driving under V_MAX_AFTERHANDOVER] Or [The train is driving over V_MAX_AFTERHANDOVER] The train engages ATO.
	Step 3.1.1	[If The train is driving over V_MAX_AFTERHANDOVER] The train starts slowing-down to some speed V_New lower than V_MAX_AFTERHANDOVER. Once this speed is reached, Branch to Step 3.1.2.
	Step 3.1.2	[The train is driving under V_MAX_AFTERHANDOVER.] The train asks RSC's lost alarm policy if it can switch to full autonomy. The lost alarm policy may agree, for instance because the train is allowed full autonomy. In that case, branch to Step4. Some lost alarm policy may set conditions for a train being not monitored. For instance, the train may have been preliminary assigned to a RUS. If the conditions set by the lost alarm policy are not met, Branch to 3.2.
	Step 3.2	In case the conditions set by the lost alarm policy to the train are not met, e.g. RUS was not assigned to the train that tries to go into autonomous operation, handover to GoA 3/4 is cancelled. Terminate use case and remain under control of RD. Note: the fact that in this use-case a RUS can be mandatory for the train to switch into unmonitored GoA4 driving does not force the RUS to be constantly monitor the train later. It just permits to determine a receiver for the lost alarm policy of the RSC. Other lost alarm policies can be imagined, where a RUS does not have to be defined – an RSC with a sound lost alarm policy is enough.
	Step 4	[The train is driving under V_MAX_AFTERHANDOVER] and [The lost alarm policy allows the handover] The handover takes place.

Postcondition	The train is now operating in fully autonomous way, either in GoA 3 or GoA4. • The autonomous max speed now is now enforced by ETCS as part of the MRSP. • The train now monitors its own vigilance and sensor status. • The train now monitors the video quality and conditions for GoA3/4 operations. RD is no longer in control of train. RUS is. • Responsible for train supervision. • Receiving video image of the track in front of the train.
Use case notes	-

UC5.4-023 Initiate handover from autonomous train by remote driver, ATO not engaged

8 DRIVING

8.1 ROUTINE DRIVING BY REMOTE DRIVER

This use case details remote train control operation by a person in the RSC. Two remote control variation can be used when controlling a train remotely from a control centre.

Variant A: Controlling. In this option, the Remote Driver controls all train control elements and is guided by the sensors and the data sent.

Variant B: Monitoring. With this option, the Remote Driver controls only the emergency brake button, plus warning devices such as the horn. Otherwise, the train runs autonomously according to the sensors and is monitored.

Use case field	Description	
ID	UC5.4-024	
Use case name	Perform routine driving by remote driver	
Main actor	Remote Driver	
Other actors	Serviceable train (Train), ATO, Perception system	
Use case summary	This use case details remote train control operation by a person in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself. It is crucial that there is working communication between the train and the control centre and that the Remote Driver has working sensors based on which the Remote Driver drives and also access to warning sound devices.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is to ensure seamless train control by a Remote Driver.	
Preconditions	The train is operated in a centralized area; ETCS is available and functional. The Train is under control of the remote driver. The communication between the train and the control centre is operational. When this use-case starts, the train is stopped Train is stopped. ATO is not engaged.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver.
	Unsuccessful outcomes	The train is unsuccessfully controlled by a Remote Driver.
Condition affecting termination outcome	**Outcome 2**	Communication failure. No Remote Driver is available in the centre Technical failure in remote operation centre
Use case description	**Step 1**	The Remote Driver checks the functionality of individual parts of a stationary train (see UC5.4-012 for the tests).

	Step 2	The train starts. The Remote Driver attends the train motion. • Variant B Monitoring: the train is controlled by its autonomous services (a.o. ATO) or by a fellow driver. Consider steps 3.x only. • Variant A Controlling: the train is controlled by the driver himself/herself. Consider steps 3.x and 4.x.
	Variant B and A	**Services available while Monitoring and Controlling**
	Step 3	Variant B and A: The Remote Driver monitors the train motion without influence most of the time. He/she may perform one of the 3.x actions especially in case an event enters the train's lauding gauge:
	Step 3.1	The Remote Driver decreases the train's speed: controls the train's brakes lever.
	Step 3.2	The Remote Driver uses the emergency brake button to stop the train in a potential danger situation.
	Step 3.3	The Remote Driver uses warning sound devices: sounds the horn.
	Variant A only	**Services available while controlling only**
	Step 4	The Remote Driver controls the train remotely by performing all along the drive, successively or in parallel, the 4.x actions: (See also steps 3.x).
	Step 4.1	At Standstill, select / revert the driving direction: showing video and sensors of an extremity cabin or the other. Note: if the driver relies on some movement authority or journey, the default driving direction is toward the supervised location or the next stopping point. When the driver selects jogging, the focus of track sensors automatically changes – with the HMI making clear that the train is driving against expectations by IM operations.
	Step 4.2	The Remote Driver engages or disengages ATO.
	Step 4.2	The Remote Driver corrects the train's speed (controls the train's traction and brakes). Note: some assistance may permit the driver to enter a cruising speed, or a controlled acceleration maneuver, even if ATO is not engaged.
	Step 4.3	The Remote Driver confirms its vitality while driving by pressing the vitality button (UC5.4-017).
	Step 4.4	The Remote Driver manages doors. Note: some assistance may warn the train before opening the doors at a location other than in front of a platform
	Step 4.5	The Remote Driver manages external lights.

	Step 4.6	The Remote Driver manages pantographs. Note: some assistance may manage the pantographs for the driver also if he/she has not engaged ATO.
	Step 4.7	The Remote Driver wipe and wash front window and sensors, also defrost and demist front window and sensors.
	Step 4.8	The Remote Driver provides Energy for traction and auxiliaries.
	Step 4.9	The Remote Driver closes High Voltage Circuit Braker.
	Step 4.10	The Remote Driver engages the train holding brake.
	Step 5	The Remote Driver stops the train at a safe place.
	Step 6	Terminate use case.
Postcondition	The Remote Driver successfully stops the train at a safe place, where he/she will transfer responsibility for the train to the supervisor. Train remains at standstill.	
Use case notes	-	

UC5.4-024 Perform routine driving by remote driver

8.2 Driving From Yard To Platform

The operational use cases in this section try to focus to the specific actions linked to moving the train from depot to station (platform): train registration (UC5.4-001, UC5.4-007), remote control activation (e.g., UC5.4-014, UC5.4-022) and driving actions (UC5.4-024) are already defined in others uses cases.

There are two scenarios:

1 Train is transferred to a track free of occupation;
2 Train is transferred to an occupied track:
   a. To stop upstream the train occupying the track;
   b. To perform coupling with the train occupying the track

Next figure presents the use case context for both UC5.4-025 and UC5.4-026:

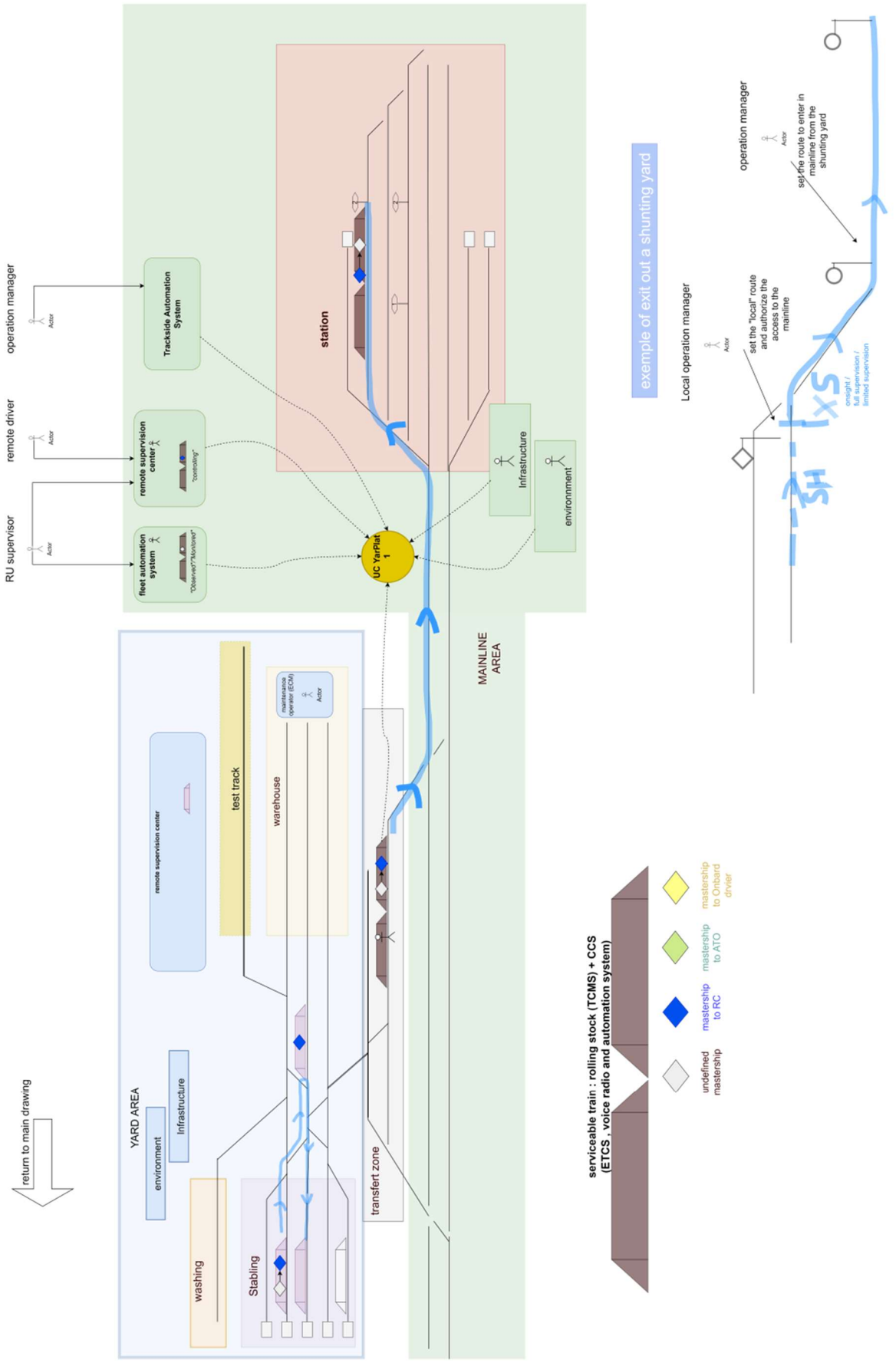

Figure 15: Context for the scenario mover from yard to platform

8.2.1 Move Train From Yard To Platform By Remote Driver– Free Track

In this variant, the train movement aims at a track free of occupation:

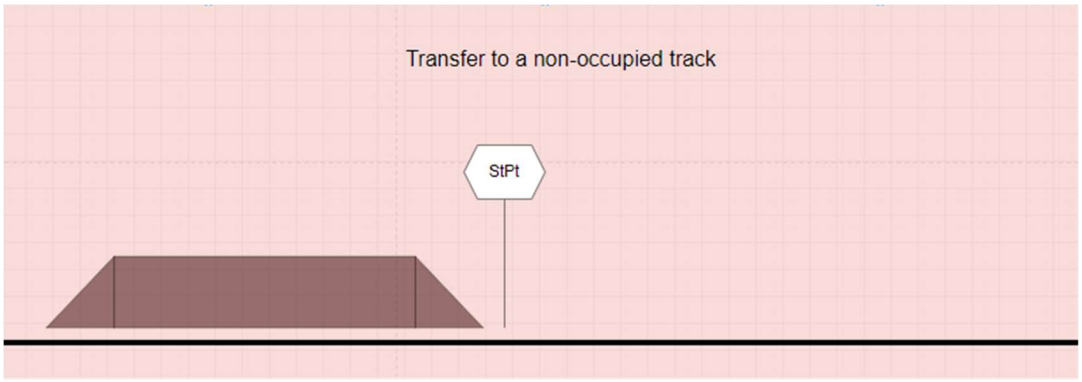

Figure 16: Transfer to a non-occupied track

Use case field	Description	
ID	UC5.4-025	
Use case name	Move train from yard to platform by remote driver– free track	
Main actor	Remote Driver (RD)	
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Serviceable Train (Train), Remote Supervision Centre (RSC), Fleet Management System (FMS)	
Use case summary	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Move the train from the depot area (“transfer zone”) to the platform where the journey will start and put the train in a condition to enable the control by the relevant user (ATO, On-board driver, Remote Driver).	
Preconditions	Train is registered to the RSC (see UC5.4-001). RUS has established the Remote Driving mission and has selected the Remote Driver in charge of the mission (UC TAURO D2.1 3.1.1) The RD controls (user registration = “controlling”) the train after UC5.4-010 and U UC5.4-012. The train is stopped in front of the exit signal (See for instance UC5.4-030: move a train in shunting yard). RD has previously entered in all necessary data (see UC5.4-013 Start of mission). The train operations level is 'operative'.	
Termination outcome	**Successful outcomes**	Outcome 1: Train is at the position to start its journey and is in a configuration to be controlled by relevant user.
	Unsuccessful outcomes	Outcome 2: Remote Mission has failed due to incident (see chapter 11 p. 128 for the management of Remote Driving degraded situations).

Condition affecting termination outcome	**Outcome 2**	Loss of the remote connexion, incident during the movement.
Use case description	**Step 1**	RD: establishes communication to IOM and requests permission for route and departure.
	Step 2	IOM: confirms route and permission for departure to RD. Signal aspect switch to a permissive state and/or MA is sent to the train (ETCS).
	Step 3	Train: streams video that provides clear view to the RD (RSC driving desk) of the signal authorizing the departure of the train to enter in the main line. Alternative 1: Train provides to the RSC(RD) movement authority authorizing train movement (L2 FS/OS/SH).
	Step 4	RD: selects driving direction forward and drives remotely the train (see UC5.4-024 for detailed action). - RD: commands traction and braking to accelerate maintain speed and decelerate. - RD: commands horn, radio alert, pantograph and Emergency brake in case of incident. - RD: commands horn and headlight when crossing train. - RD acknowledges train (ETCS) message if necessary. - RD informs IOM about any incident and receives orders from IOM
	Step 5	Train: provides clear view of the platform and the stopping point position to RD.
	Step 6	RD: commands train brakes to stop the train at the correct position.
	Step 6.1	(undershooting or overshooting) RD: inform IOM about the non-accurate stop
	Step 6.1.1	RD: initiates jog movement. Note: to this intend, the track view on the Remote Driving desk focuses to the train rear.
	Step 7	RD: commands brake effort to hold the train (UC5.4-024).
	Step 8	RD: informs the RUS and IOM that mission is completed.
	Step 9	RD: releases the control of the train: RD's status toward train changes from controlling to observing or monitoring, e.g. by means of Mastership-21 or RD performs handover with the next train driver (Mastership-10, Mastership-11, , Mastership-12, Mastership-22).
Postcondition	Train at standstill at the station ready for main operation.	
Use case notes	Rely on TAURO D2.1 UC3.1.3	

UC5.4-025 Move train from yard to platform by remote driver– free track

8.2.2 Move Train From Yard To Platform – Occupied Track

In this variant, the train movement aims at a track already occupied:

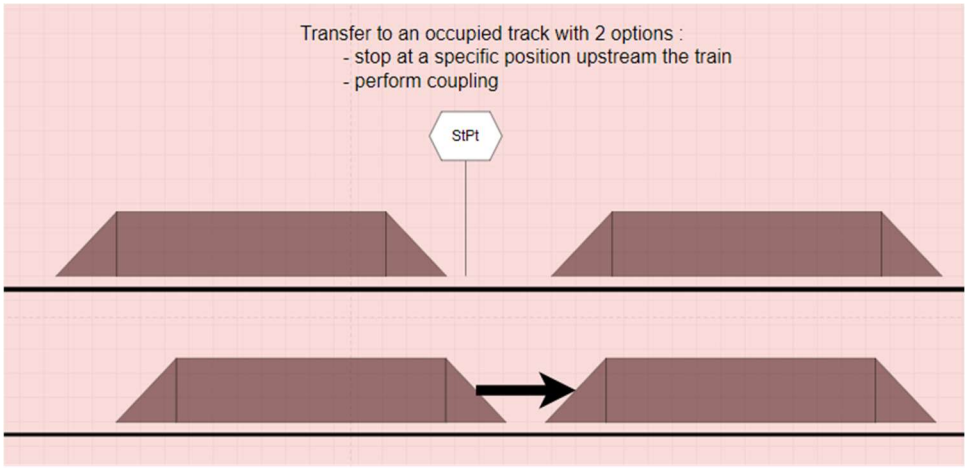

Figure 17: Move to occupied track

Use case field	Description	
ID	UC5.4-026	
Use case name	Move train from yard to platform – occupied track	
Main actor	Remote Driver (RD)	
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Serviceable Train (Train), Remote Supervision Centre (RSC), Fleet Management System (FMS)	
Use case summary	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Move the train from the depot area to the platform where the journey start, perform eventually a coupling and put the train in a condition to enable the control by the relevant user (ATO, On-board driver, Remote Driver).	
Preconditions	Train is registered to the RSC (see UC5.4-001). RUS has established the Remote Driving mission and has selected the Remote Driver in charge of the mission (UC TAURO D2.1 3.1.1). The RD controls (user registration = “controlling”) the train after UC5.4-010 and UC5.4-012. The train is stopped in front of the exit signal (See for instance UC5.4-030: move a train in shunting yard). RD has previously entered in all necessary data (see UC5.4-013 Start of Mission). The train operations level is 'operative'.	
Termination outcome	**Successful outcomes**	Outcome 1: Train is at the position to start its journey and is in a configuration (single or multiple unit) to be controlled by relevant user.

	Unsuccessful outcomes	Outcome 2: Remote Mission has failed due to incident (see UC5.4.RecContFail for the management of Remote Driving degraded situations).
Condition affecting termination outcome	**Outcome 2**	Loss of the remote connexion, incident during the movement or coupling.
Use case description	**Step 1**	RD: establishes communication to IOM and requests permission for route and departure.
	Step 2	IOM: confirms route and permission for departure to RD. Signal aspect switch to a permissive state and/or MA is sent to the train (ETCS).
	Step 3	Train: streams video that provides a clear view to the RD (RSC driving desk) of the signal authorizing the departure of the train to enter in the main line. Alternative 1: Train provides to the RSC(RD) "movement authority" authorizing train movement (L2 FS/OS/SH)'.
	Step 4	RD: selects the driving direction and drives the train (see UC5.4-024 for detailed action). - RD: commands traction and braking to accelerate maintain speed and decelerate. - RD: commands horn, radio alert, pantograph and Emergency brake in case of incident. - RD: commands horn and headlight when crossing train. - RD acknowledges train (ETCS) message if necessary. - RD informs IOM about any incident and receives orders from IOM
		Train: provides clear view of the signal indicating the track is occupied and on-sight movement is authorized within occupied track. Alternative 1: Train provides MA Onsight information
	Step 5	RD: acknowledges transition to "Onsight"
	Step 6	Train: provides clear view of the platform, the stopping point position and the train occupying the track.
	Step 7	RD: commands train brakes to stop the train.
	Step 8	Train: stops
	Step 8.1	(Coupling requested): RD performs the coupling using train capacity if needed (low speed regulation etc). Refer to UC5.2-0028 in [D5.2 UCs PER] dedicated to coupling.
	Step 8.2	(Coupling not requested) and (RD overshoot or undershoot stopping point) RD performs jog movement.
	Step 9	RD: commands train holding brake.
	Step 10	RD: informs the RUS and IOM that mission is completed.
	Step 11	RD: releases the control of the train: RD's status toward train changes from controlling to observing or monitoring, e.g. by means of Mastership-21 or RD performs handover with the next train driver (Mastership-10, Mastership-11, , Mastership-12, Mastership-22).
Postcondition	Train at standstill at the station ready for main operation.	
Use case notes	This use case relies on TAURO D2.1 UC3.1.3	

UC5.4-026 Move train from yard to platform – occupied track

8.2.3 Move Train From Platform To Yard.

Next figure presents the use case context for both UC5.4-025 and UC5.4-026:

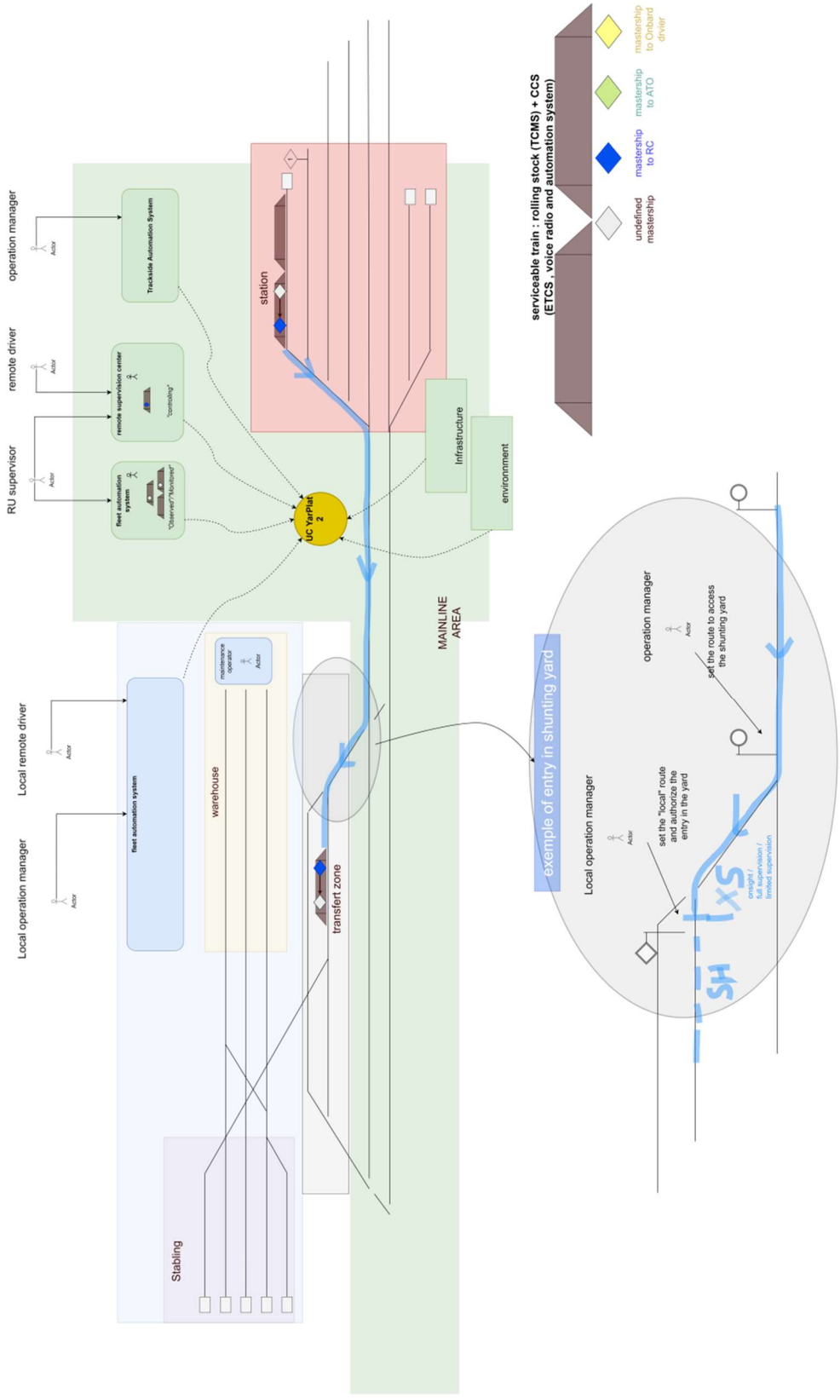

Figure 18: Context for the scenario Move from Platform to yard

Use case field	Description	
ID	UC5.4-027	
Use case name	Move train from platform to yard.	
Main actor	Remote Driver (RD).	
Other actors	IM Operations Manager (IOM), Local Operational Manager (LOP), Railway Undertaking Supervisor (RUS), Serviceable Train (Train), Remote Supervision Centre (RSC), Fleet Management System (FMS)	
Use case summary	The Remote Driver takes the responsibility for moving the train from Yard to Platform.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Move the train from the station to the yard (“transfer zone”) where local user will take in charge the control of the train (remotely, manually or automatically).	
Preconditions	Train is registered to the RSC (see UC5.4-001). RUS has established the Remote Driving mission and has selected the Remote Driver (RD) in charge of the mission (UC TAURO D2.1 3.1.1). The RD controls (user registration = “controlling”) the train (handover with previous user if any: see UC5.4-010 and UC5.4-012). Train is stopped at the station. The train operations level is 'operative': Train provides to the RD the views of the cabin directed to the yard.	
Termination outcome	**Successful outcomes**	Outcome 1: Train in the yard at the requested position and in a configuration to be controlled by relevant user.
	Unsuccessful outcomes	Outcome 2: Remote Mission has failed due to incident (see for instance UC5.4.RecContFail-1 and -2 for the management of Remote Driving degraded situations).
Condition affecting termination outcome	**Outcome 2**	Loss of the remote connexion, incident during the movement.
Use case description	**Step 1**	(mission request uncoupling) RD: perform uncoupling
	Step 2	RD: enter driver id and perform ETCS data entry if needed.
	Step 3	RD: select the driving mode (SH,SR) if needed.
	Step 4	RD: establish communication to IOM and requests permission for route and departure.
	Step 5	IOM: confirms route and permission for departure to RD. Signal aspect switch to a permissive state and/or MA is sent to the train (ETCS).
	Step 6	Train: provides clear view to the RD of the signal authorizing the departure of the train. Alternative 1: Train provides to the RD movement authority authorizing train movement (L2 FS/OS/SH).

	Step 7	RD: selects driving direction forward and drives remotely the train (see UC driving for detailed action). - RD: commands traction and braking to accelerate maintain speed and decelerate. - RD: commands horn, radio alert, pantograph and Emergency brake in case of incident. - RD: commands horn and headlight when crossing train. - RD: acknowledges train (ETCS) message if necessary. - RD: command the life sign. - RD informs IOM about any incident and receives orders from IOM
	Step 8	Train: provides clear view of signal indicating the direction is set to enter shunting yard.
	Step 9	RD: establishes communication with local operational manager (LOP)
	Step 10	LOP: gives to RD authorization to enter in the yard.
	Step 11	(Train not in shunting) Train: provides ETCS display to RD with the request to acknowledge the transition to shunting mode.
	Step 11	RD: acknowledge ETCS SH mode when passing the yard entry point.
	Step 12	Train provides to RD clear view of the track and the position where RD shall stop the train.
	Step 13	RD: stop the train at the requested stopping position.
	Step 14	RD: commands brake effort to hold the train (UC5.4-024).
	Step 15	RD: set the train to a mode for the next mission (service retention, sleep etc.)
	Step 16	RD: informs the RUS and IOM that mission is completed.
	Step 17	RD: releases the control of the train: RD's status toward train changes from controlling to observing or monitoring, e.g. by means of Mastership-21 or RD performs handover with the next train driver (Mastership-10, Mastership-11, Mastership-12, Mastership-22).
Postcondition	Train at standstill in the shunting yard.	
Use case notes	Rely on TAURO D2.1 UC3.1.3	

UC5.4-027 Move train from platform to yard.

8.3 DEPOT MANOEUVERS

8.3.1 Move The Train In Depot For Train Composition By Remote Driver

Use case field	Description
ID	UC5.4-028
Use case name	Move the train in depot for train composition by remote driver
Main actor	Remote Driver
Other actors	Serviceable train (Train), ATO, Perception system
Use case summary	This use case details remote train control operation in depot by a person in the control centre.

	The Remote Driver should be able to drive the train remotely as if on the train itself. It is crucial that there is working communication between the train and the control centre and that the Remote Driver has working sensors based on which the Remote Driver drives and also access to warning sound devices.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is to ensure seamless train control by a Remote Driver in depot.	
Preconditions	1. Train is under control of local train driver OR GoA3/4 OR Train is in shutdown mode, but mobile connection to RU is open. 2. Train has all tracking devices working. 3. Train is stopped. 4. Communication between the train and the control centre is operational. 5. The Remote Driver checks that all systems and train controls are functioning. 6. Train is operated in a depot.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver.
	Unsuccessful outcomes	The train is unsuccessfully controlled by a Remote Driver.
Condition affecting termination outcome	**Outcome 2**	Communication failure. No Remote Driver is available in the centre Technical failure in remote operation centre
Use case description	**Step 1**	The Remote Driver checks the functionality of individual parts of a stationary train (see UC5.4-012 for the tests).
	Step 2	The train starts. The Remote Driver attends the train motion. • Variant B Monitoring: the train is controlled by its autonomous services (a.o. ATO) or by a fellow driver. Consider steps 3.x only. • Variant A Controlling: the train is controlled by the driver . Consider steps 3.x and 4.x.
		Safety relevant services
	Step 3	The Remote Driver may perform one of the 3.x actions especially in case an event enters the train's lauding gauge:
	Step 3.1	The Remote Driver decreases the train's speed: controls the train's brakes lever.
	Step 3.2	The Remote Driver uses the emergency brake button to stop the train in a potential danger situation.

	Step 3.3	The Remote Driver uses warning sound devices: sounds the horn.
	Variant A only	**Services available while controlling only**
	Step 4	The Remote Driver controls the train remotely by performing all along the drive, successively or in parallel, the 4.x actions: (See also steps 3.x).
	Step 4.1	At Standstill, select / revert the driving direction: showing video and sensors of an extremity cabin or the other. Note: if the driver relies on some movement authority or journey, the default driving direction is toward the supervised location or the next stopping point. When the driver selects jogging, the focus of track sensors automatically changes – with the HMI making clear that the train is driving against expectations by IM operations.
	Step 4.2	The Remote Driver engages or disengages ATO.
	Step 4.2	The Remote Driver corrects the train's speed (controls the train's traction and brakes). Note: some assistance may permit the driver to enter a cruising speed, or a controlled acceleration manoeuvre, even if ATO is not engaged.
	Step 4.3	The Remote Driver confirms its vitality while driving by pressing the vitality button (UC5.4-017).
	Step 4.4	The Remote Driver manages doors. Note: some assistance may warn the train before opening the doors at a location other than in front of a platform
	Step 4.5	The Remote Driver manages external lights.
	Step 4.6	The Remote Driver manages pantographs. Note: some assistance may manage the pantographs for the driver also if he/she has not engaged ATO.
	Step 4.7	The Remote Driver wipe and wash front window and sensors, also defrost and demist front window and sensors.
	Step 4.8	The Remote Driver provides Energy for traction and auxiliaries.
	Step 4.9	The Remote Driver closes High Voltage Circuit Braker.
	Step 4.10	The Remote Driver engages the train holding brake.
	Step 5	The Remote Driver stops the train at a safe place in depot.
	Step 6	Terminate use case.
Postcondition	The Remote Driver successfully stops the train at a safe place, where he/she will transfer responsibility for the train to the supervisor. Train remains at standstill.	
Use case notes	-	

UC5.4-028 Move the train in depot for train composition by remote driver

8.4 SHUNTING YARDS

UC5.4-029 represents a movement in the shunting yard, while UC5.4-030 permits to handover to some shunting personnel. This shunting personnel drives while the locomotive is pushing the train. He/she drives from the pedestrian platform on the last wagon and at the train extremity. In this activity, the shunting personnel is considered a pedestrian driver (see section 3.1 p.26 and chapter 9 p.119).

8.4.1 Shunt In Centralized Area

Shunting can be performed in a centralized area: coordinated with the help of some technical equipment, typically occupancy detection and signalling, according to standardised rules of operation. It may also be performed in non-centrally controlled areas. For instance, the 2 tracks constituting the loading/unloading area on the private network of a gravel mine may be so simple, that an interlocking is not necessary. Next use case assumes a centralized area.

Important note: the speed limit in the UC is not our proposal for a standardized shunting speed, but an example of one national situation - and that this maximum is depending on national rules and underlying signalling systems. The maximum speed of 30 km/h is valid for some countries for others 40 km/h is used. Similarly for the associated restrictions, aren't the same in every countries. This is an example on how Remote Driving can work.

Use case field	Description	
ID	UC5.4-029	
Use case name	Shunt in centralized area	
Main actor	Remote Driver (RD)	
Other actors	Remote Supervision Centre (RSC) Centralized Trackside Automation System (TAS) On-board Automation System (OAS)	
Use case summary	Driving the train in a centralized area (shunting). The train is driven remotely by a Remote Driver. Maximum speed 30 km/h.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The train can be driven (shunting) by RD from some RSC while the train is located inside a centralized area.	
Preconditions	Vehicle is operated in a centralized area with some RSC. Remote operation is an independent system (from ATO) RD is monitoring the train, or has control over the vehicle. The vehicle is at standstill.	
Termination outcome	**Successful outcomes**	Outcome 1: The Train gets to the location defined by RD and can perform coupling/uncoupling activity
	Unsuccessful outcomes	Outcome 2: Technical problems on the train prevent remote driving.

		Outcome 3: RD cannot determine the signal aspects required for driving Outcome 4: Mobile connection is too bad to allow safe remote operation
Condition affecting termination outcome	**Outcome 2-4**	Explanations: Outcome 2: RD cannot drive. Outcome 3: RD cannot determine the signal aspects required for driving. This can be due to unknown position, bad weather or camera range. Outcome 4: Due the bad mobile connection, the journey cannot continue (safety relevant) Postconditions: Outcome 2-3: Train remains in standstill. RSC requests FAS to send on-site on-board driver to train. Outcome 4: OAS stops train and prevents remote operation until connection is good again. FAS may send local on-board driver, if the connection is not recovering.
Use case description	**Step 0**	[RD is monitoring the train. If he/she has control already, Branch to step 2] RD gets control over vehicle (Use case UC5.4-030)
	Step 1	RD checks the health of the vehicle including necessary brake tests.
	Step 1.1	If the train has technical problems (defect brakes, pantograph, motors etc), branch to Outcome 2.
	Step 2	[RD has control over the train already] RD selects shunting mode
	Step 2 a	OAS applies a speed limit of 30 km/h for shunting.
	Step 3	RD assures the position where the vehicle is and reads the signal aspects
	Step 3.1	If RD does not know where he is and/or cannot determine the signal aspects, branch to Outcome 3
	Step 4	Optionally: if regulation requires a clearance from the operations centre, RD calls operation centre to get the clearance. RD waits for clearance
	Step 4 a	Operation centre sets the route.
	Step 5	RD waits for signal aspect allowing driving
	Step 6	RD moves the vehicle to the planned position obeying the regulations for this track and type of train.
	Step 6.1	At any time during the shunting operation: If the remote connection is “too bad” (the necessary quality of the connection has to be defined using tests and human factor analyses), the OAS on the train stops the train and prevents remote operation until the connection is “good” again. Branch to Outcome 4 For details, please refer to 12, Degraded Modes Specific to Remote Control, p.141.

	Step 6.2	At any time during the shunting operation: if RD cannot obey the regulation rules (e.g., cannot see signals, obstacles on track, etc.), RD initiates an emergency stop of the vehicle. He can continue if the regulations can be obeyed again.
	Step 7	Train arrives at its supposed destination.
	Step 8	Optionally: perform coupling operations
	Step 9	Optionally: RD may activate the other cabin and continue driving in the other direction. Branch to Step 1
Postcondition	Train is under control of RD and may execute another movement.	
Use case notes	This use case assumes a maximal shunting speed of 30km/h. Some countries/operators may choose another value, e.g.40 km/h	

UC5.4-029 Shunt in centralized area

8.4.2 Handover For Push Movement In Shunting

Use case field	Description
ID	UC5.4-030
Use case name	Handover for push movement in shunting
Main actor	Remote Driver (RD)
Other actors	Remote Supervision Centre (RSC), for instance a local one dedicated to shunting Shunting Personal taking the role of a Pedestrian driver (SHPD) Fleet Management System (FMS) Serviceable Train (Train) and its On-board Automation System (OAS)
Use case summary	Remote operation in shunting. A maximum shunting speed of 30 km/h is assumed.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	Provide shunting by remote operation. Remote operation here is a Remote Driver in the RSC. No local staff with a remote control. This use case only describes the handover to a Remote Driver. The actual driving is described in use case UC5.4-029.
Preconditions	Train is operated in a centralized area. Train is at standstill, operative. RSC is alive Remote Driver RD available in RSC. Remote Driver is monitoring or controlling (also driving) the train from a remote cabin.

	Shunting Personal SHPD is observing the train (Pedestrian HMI) and lying along the track, close to the train.	
Termination outcome	**Successful outcomes**	• Outcome 1: SHPD has control over train and can perform shunting operations. After his operations, he gives back control to OAS or to RD or the train is switched to service retention mode.
	Unsuccessful outcomes	• Outcome 2: No Remote Driver available • Outcome 3: Mobile connection fails or has not the necessary quality • Outcome 4: Remote operation system failure
Condition affecting termination outcome	**Outcome 2**	Explanations: Outcome 2: No Remote Driver is available in the centre. Wait for Remote Driver to be available. Outcome 3: If the mobile connection is of bad quality (jitter, bandwidth), the OAS stops the train. Outcome 4: Technical failure in remote operation centre. Postconditions: Outcome 2: Train remains at standstill. Remote operation centre asks FMS to send local driver to train. Outcome 3: Train remains at standstill until mobile connection is of good quality again. Remote operation centre asks FMS to send a local driver to train if the problem is persistent. Outcome 4: Remote operation centre asks FMS to send local driver to train. Train remains at standstill.
Use case description	**Step 0**	[Optional: RD is monitoring the train. If RD is controlling the train already, Branch to step 1] RD requests remote operation centre for Remote Driver to take over control (see UC5.4-019).
	Step 0.1	[RD is controlling the train] In case of no response of Remote operation centre, branch to Outcome 4
	Step 1	[Option: SHPD is not yet monitoring the train] The Shunting personnel SHPD is observing the vehicle to which he/she wants to connect (Pedestrian HMI). SHPD (shunting mode) selects the vehicle to which he/she wants to connect. The train grants “Monitoring” status to SHPD.
	Step 1.1	[SHPD is monitoring the train already] SHPD requests control (see UC5.4-031, UC5.4-032, UC5.4-033). In case of success
	Step 1.2	If the connection fails – Branch to Outcome 4
	Step 2	OAS grants access to SHPD.

		Note: OAS has checked the handover conditions, incl. the fact that the train is at standstill, which is mandatory for a handover by a pedestrian driver. Train speed is limited to shunting speed 30 km/h.
	Step 3	SHPD selects the orientation of his/her control to pushing due to shunting. SHPD climbs on the platform at the train extremity on the side opposite to the locomotive.
	Step 4	SHPD: moves train from his/her platform for pushing manoeuvres – see UC5.4-033.
	Step 5	RD: initiates handover from SHPD (see UC5.4-020). Train speed is limited to shunting speed 30 km/h.
	Step 6	RD: operates the train (see UC5.4-029) for pulling manoeuvres.
	Step 5.1	If mobile connection quality is not sufficient to operate remotely: OAS stops train. Branch to Outcome 3
	Step 6	SHPD: closes the session and gives control back to RD
Postcondition	Train is under control of RD, ready for Start Of Mission procedure with new wagons (UC5.4-013).	
Use case notes	-	

UC5.4-030 Handover for push movement in shunting

9 PEDESTRIAN DRIVER

Pedestrian drivers may be some Emergency Manager (see [SRS X2Rail-4 v0.3.0], section 9.4), some Maintenance Depot Pedestrian Driver or some Shunting Operator. They are shown in Figure 2: Operational entities and actors directly involved in remote , p.27.

From the point of view of remote control, they share the task to move a train at low speed, while being placed in the vicinity of the train's front (extremity in the direction of movement). According to their role some specificities:

Shunting: driving while a freight train is pushing. Frequent hand-over with an on-board driver or a remote driver in some RSC for pulling. Driving from the pedestrian platform on the last wagons and located at the train extremity.

Emergency manager: movement limited to a distance sufficient to free a person or body trapped under the train, inspect an axle ([SRS X2Rail-4 v0.3.0] section 7.10.3 local Control, [SRS X2Rail-4 v0.3.0] section13.7.6 Move the train locally).

Depot Pedestrian Driver: movement in the depot. May have to be limited by systems locking the train while under maintenance.

The use-case in this chapter present the interactions between trains and drivers common to those profiles.

9.1 INITIATE HANDOVER FROM REMOTE PEDESTRIAN DRIVER

Shunting personnel may need to give/take control to/from the driver responsible for pulling several times during a shunting series (on-board, remote). Some emergency manager may request control from the remote driver assigned to a common incident. And a Depot pedestrian driver at an extremity may request control from another at the other extremity of the train while adjusting the train's exact stopping position.

A driver is taken exemplarily as initially controlling the train.

Use case field	Description
ID	UC5.4-031
Use case name	Initiate handover by pedestrian remote driver
Main actor	Pedestrian driver PD
Other actors	Remote Driver RD, Serviceable train (Train)
Use case summary	A pedestrian driver claims responsibility for a train. The remote driver who was in control grants the responsibility.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles

Main goal	Illustrate how a pedestrian driver claims responsibility from another driver. As an example, the other driver is a remote driver. He/she could have been an on-board or another pedestrian driver.	
Preconditions	The train is at standstill. RD in a remote-control centre is in control of the train. PD is less than 10m away from one the extremities of the train. PD is equipped with some pedestrian driver HMI: tablet or smartphone, or some dedicated system with joysticks and/or screens (Figure 7 p.36). PD is monitoring the train.	
Termination outcome	**Successful outcomes**	PD is controlling the train.
	Unsuccessful outcomes	Neiter RD nor PD is controlling the train
Condition affecting termination outcome	**Outcome 2**	RD is still controlling the train
Use case description	**Step 1**	PD issues a RemoteControlRequest by pushing the button RSC-ClaimGrant on his/her interface. The pedestrian HMI computes a maximum speed V_Max_Driver function of PD's accreditation profile and location (area of the accreditation). It sends a HandoverRequest (V_Max_Driver, PedestrianPositionLatLong) to the train.
	Step 2	The train receives the HandoverRequest from PD. It verifies that it is at standstill. If not, it refuses the request, as PD is a pedestrian driver. The use case ends with outcome 2. It computes the distance from the driver to the train. If this distance is more than 10 meters, the train refuses the request. The use case ends with outcome 2. If this distance is less than 10 meters, the train computes a maximum speed it allows for the driver. This results in V_MAX_AFTERHANDOVER. The train notifies RD that PD requests for control.
	Step 3.1	An alarm at RD's workplace that means 'request to take-over by pedestrian driver'. RD may decide: 1. [RD refuses or ignores the claim.] Branch to 3.1.1 2. [RD confirms the handover] Branch to 3.1.2
	Step 3.1.1	[RD refuses or ignores the claim.]

		After a time-out, PD gets on his/her HMI a dialog 'HandOverRequest IgnoredOrRejected'. The use case finishes as Outcome2. Note: The drivers may discuss their reasons on the voice channel. After this, the use case may be re-entered.
	Step 3.1.2	[RD confirms the handover] The handover takes place. Branch to postconditions.
Postcondition	PD is now Controlling the train. RD is now Monitoring the train.	
Use case notes	-	

UC5.4-031 Initiate handover by pedestrian remote driver

9.2 INITIATE HANDOVER FROM PEDESTRIAN DRIVER

Use case field	Description	
ID	UC5.4-032	
Use case name	Initiate handover by pedestrian driver	
Main actor	Pedestrian driver PD1	
Other actors	Other pedestrian driver PD2, Serviceable train (Train)	
Use case summary	A pedestrian driver claims responsibility for a train currently under responsibility of another pedestrian driver. The pedestrian driver who was in control grants the responsibility to the other.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Illustrate how a pedestrian driver grants responsibility to another driver. As an example, the other driver is a pedestrian driver. He/she could have been an on-board or Remote Driver.	
Preconditions	The train is at standstill. PD2 is in control of the train. PD1, is less than 10m away from one the extremities of the train. The pedestrian drivers are equipped with some pedestrian driver HMI: tablet or smartphone, some dedicated system with joysticks and/or screens.	
Termination outcome	**Successful outcomes**	PD1 is controlling the train.

	Unsuccessful outcomes	Neiter PD1 nor PD2 is controlling the train
Condition affecting termination outcome	**Outcome 2**	PD2 is still controlling the train
Use case description	**Step 1**	PD1 issues a RemoteControlRequest by pushing the button RSC-ClaimGrant on his/her interface. The workplace computes a maximum speed V_Max_Driver for the driver function of: • He/she is a pedestrian driver • Where he/she lies (latitude, longitude). It sends a HandoverRequest (V_Max_Driver, PedestrianPositionLatLong).
	Step 2	The train receives the claim PD1. It verifies that it is at standstill. If not, it refuses the request. The use case ends with outcome 2. It computes the distance from the driver to the train. If this distance is more than 10 meters, it refuses the request. The use case ends with outcome 2. If this distance is less than 10 meters, the train computes a maximum speed it allows for the driver PD1. This results in V_MAX_AFTERHANDOVER.
	Step 3.1	A bell rings at PD2's HMI, that means 'request to take-over by PD1'. PD2 may decide: 1. [PD2 refuses or ignores the claim.] Branch to 3.1.1 2. [PD2 confirms] Branch to 3.1.2
	Step 3.1.1	[PD2 ignores the claim.] After a time-out, PD1 gets on its HMI a dialog 'HandOverRequest IgnoredOrRejected'. The use case finishes as Outcome2. Note: The drivers may discuss their reasons on the voice channel. After this, the use case may be re-entered.
	Step 3.1.2	[PD2 confirms handover] The handover takes place. Branch to postconditions.
Postcondition	PD1 is now Controlling the train. PD2 is now Monitoring the train.	
Use case notes	-	

UC5.4-032 Initiate handover by pedestrian driver

9.3 MOVE THE TRAIN LOCALLY BY PEDESTRIAN DRIVER

Use case field	Description	
ID	UC5.4-033	
Use case name	Move the train locally by pedestrian driver	
Main actor	Pedestrian driver	
Other actors	Serviceable train (Train)	
Use case summary	The pedestrian driver moves the train in creeping speed and controls the traction power.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	This use case intends to enable the local control of a train by trackside staff	
Preconditions	The pedestrian driver is controlling the train – as a result of UC5.4-031 or UC5.4-032. The traffic is supposed sufficiently secured around the driver for him/her to concentrate on driving the train without hazard for his/her life: • Maintenance depot has no traffic around • Shunting: the pedestrian driver is on the last wagon's pedestrian platform located to the end of the train • Open track: Operations Management has secured the traffic around the driver	
Termination outcome	**Successful outcomes**	The train is moving with creeping speed.
	Unsuccessful outcomes	The train is galloping.
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1**	The pedestrian driver may perform any of the following steps: 2.x, ...
	Step 2.1	The pedestrian driver defines the direction of its next driving command. The pedestrian may perform any of following Steps: 2.2, 2.3
	Step 2.2	The pedestrian driver commands the train 'Creep with constant speed'. This command may permit to disengage the train after a collision (Emergency Manager), to position it precisely in a depot (Maintenance pedestrian driver). Note: if supervised by ETCS-OB, the train makes sure it does not leave its movement authority (Emergency Manager).

		Note: If in a depot, the train may make sure it does not hit buffers (Maintenance driver).
	Step 2.3	The pedestrian driver commands the train 'Wheel Rotation'. This command permits to check axles. It is complementary to step2.2. The movement is not controlled according to speed regulation, but moved distance.
	Step 3	The pedestrian driver raises the Pantograph
	Step 4.1	The pedestrian driver lowers the Pantograph
	Step 4.2	The pedestrian driver closes High Voltage Circuit Brakers
	Step 4.3	The pedestrian driver stops the train
Postcondition	The train is stopped, somewhere else.	
Use case notes	See also UC.5.1.0825.	

UC5.4-033 Move the train locally by pedestrian driver

10 TRANSVERSE TOPICS

10.1 UC5.4-034 WARN ITS ENVIRONMENT BY THE STARTING TRAIN

Use case field	Description	
ID	UC5.4-034	
Use case name	Warn its environment by the starting train	
Main actor	Serviceable train (Train)	
Other actors	Pedestrian on track	
Use case summary	A Remote Driver monitoring a train claims responsibility for the train. The train, that was driving autonomously, creates the conditions for the take-over. The take-over takes place.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Enhance acceptancy of autonomous driving among railway professionals on the track.	
Preconditions	The train is driving autonomously or is remotely controlled– incl. ATO. The train is equipped with a pedestrian warning box (Figure 10 p.41) on each side, especially at the extremity. The train is stopped. The pedestrian warning box state is ‘Standstill’.	
Termination outcome	**Successful outcomes**	The train continues its course. No pedestrian has been harmed, also not those about to cross the train’s path.
	Unsuccessful outcomes	Catastrophic: the train has hit a pedestrian Unwished: a pedestrian has been surprised and frightened by a train with unexpected motion.
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1**	The train makes the decision / is given the order to start. The pedestrian warning boxes shift to state ‘Imminent Motion’. All cabin on-boarding boxes shift to ‘Imminent Motion’.
	Step 2	The train loosens brakes. The pedestrian warning box state shifts to ‘Motion started’. All cabin on-boarding boxes shift to ‘Don’t board’.
	Step 3	The train speed reaches 15 km/h. The pedestrian warning box shift to ‘Motion established’ External cabin on-boarding boxes shift to ‘off’.

Postcondition	The train is moving. Pedestrians have had the opportunity to detect the start of its motion before its motion was fast enough to be easily detectable.
Use case notes	UC5.4-015 and UC5.4-016 are related. UC5.4-034 Warn its environment by the starting train

10.2 UC5.4-035 BOARD A TRAIN BY DRIVER

Use case field	Description	
ID	UC5.4-035	
Use case name	Board a train by driver.	
Main actor	On-board Driver	
Other actors	Serviceable train (Train), The boarding boxes of one of its cabin doors.	
Use case summary	An on-board driver wants to board on or off a train. the on-board driver locks train motion by pushing the button on the door's boarding box at the on-board driver side. Once finished with boarding. the on-board driver releases the train motion by pushing again the button on the boarding box at onboard driver side. Several start conditions are gathered: train ready to board, already booked for motion, ...	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Ensure the safety of the driver also if the train decides to start against his/her expectations.	
Preconditions	The train is at standstill. The train maybe autonomous, remotely monitored or remotely controlled.	
Termination outcome	**Successful outcomes**	The On-board Driver has boarded the train.
	Unsuccessful outcomes	The Driver has not boarded the train.
Condition affecting termination outcome	**Outcome 2**	Initial train speed. Competence profile of the Remote Driver.
Use case description	**Step 1**	The driver approaches a cabin door to board on a locomotive. According to the state of the door's on-boarding box, jump to different steps: • Door available for reservation: Step 2.x • Door unavailable: Step 3.x • Door reserved for boarding: 4.x • Imminent motion: 5.x

	Step 2	Boarding box was in state 'Door available for reservation': He/she pushes the on-boarding box's button. The train sets all boarding boxes associated to the door in state 'Door available for reservation'. The train locks its motion until the push button of one of the two on-boarding boxes of the door is pushed again.
	Step 2.1	The driver boards
	Step 2.2	The driver pushes the button on the other side of the door. The train sets all boarding boxes associated to the door in state 'Door available for reservation' The train unlocks its motion if boarding box of any door is in state 'Door reserved for boarding'. Note: several drivers may have used several doors at the same time without seeing each other.
	Step 3	Boarding box was in state 'Door unavailable': If the driver pushes the button, the push is ignored. The driver shall stay not start boarding on. Should the driver try to board (climb the ladder), his/her safety is not guaranteed. The use case ends.
	Step 4	Boarding box was in state 'Door reserved for boarding'. The driver does not know why the door is already reserved for boards. He/she boards without pushing the button: this would release the door and potentially, the train motion. Once in the cabin, once he/she has made sure nobody else requires that the train motion is locked, he/she may release the door (Step 2.2).
	Step 5	Boarding box was in state 'Imminent motion'- The driver shall keep away from the train. If he/she pushes the boarding button, it is ignored by the train.
Postcondition	The driver is safe, either on the train or on the track.	
Use case notes	UC5.4-015 and UC5.4-016 are related.	

UC5.4-035 Board a train by driver.

11 ADDRESSING DEGRADED MODES OF THE AUTONOMOUS TRAIN

11.1 ATO IN FAULT

In next 2 scenarios, a remote driver takes the control of a train affected by a loss of its ATO component (X2Rail-4: ADM) and previously running in GoA3 or GoA4 respectively.

In the GoA3 variant, the train simply starts with braking. In the GoA4 variant, advantage is taken that the safety components are still available (obstacle avoidance, train protection): train first coasts to give the time to a driver to take-over.

Please also consider use-case TAURO UC3.1.0.6 in [SRS TAURO 08] where ATO is deactivate/isolated before manual driving.

11.1.1 Take Responsibility Of A GoA3 Train With Degraded ATO By Remote Driver

Use case field	Description	
ID	UC5.4-036	
Use case name	Take responsibility of a GoA3 train with degraded ATO by remote driver	
Main actor	On-board Automation System (OAS)	
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Remote Driver (RD)	
Use case summary	The train is originally in GoA3. The ATO is in fault and the Remote Driver takes responsibility for the train (*1)	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is to manage the ATO degraded condition by a Remote Driver and minimize delays.	
Preconditions	Train is equipped with RTO components and full functional except ATO for GoA4 operation. <u>The train is registered at some RSC it reports to.</u> "High availability of ETCS is mandatory for GoA3/4 operation (remote control is not possible if ETCS is in SF mode)." SRS 0.3.0 10.6 "(TCMS-12) GoA3/4 exported constraint: In remote control mode, TCMS shall act directly on traction or brakes (bypass of Train Protection or ADM commands)." SRS 0.3.0. 11.16.12 "(TUM-7.4) GoA3/4 exported constraint: Remote control shall be performed under ETCS supervision. Remote control shall not be possible when ETCS is in SF mode." SRS 0.3.0 12.18.7	
Termination outcome	**Successful outcomes**	Outcome 1: Train can continue. The train is successfully controlled by a Remote Driver. Delay can be minimized.

	Unsuccessful outcomes	The train cannot be remotely controlled. A driver must come to the train and take control of the train from the cabin. A driver must enter the train and takes control of the train
Condition affecting termination outcome	**Outcome 2**	Train can drive with reduced speed.
Use case description	**Step 1**	OAS: Detect failure of automatic speed control function and change from AD to FS mode (ETCS).
	Step 2	OAS: Apply brakes until train is at standstill and immobilize train with the cabin remaining virtually activated and perception function and related reactions remain active. RD is able to take over the train without going through ATO.
	Step 3	OAS: Report stopping of the train and the failure of automatic speed control to trackside automation system TAS with the request for manual train control.
	Step 4	TAS: Inform IM operations manager IOM and RUS about the stopping and the failure.
	Step 5	OAS: Inform passengers about the situation and not to leave the train.
	Step 6	RUS: Inform Remote Driver RD about the stalled train and request him to drive the train manually from remote. (e.g. UC5.4-024). Note: An ATO reset/restart could have been done in a previous state by OAS itself.
	Step 7	RD: Confirms the request from OAS to take over control of the stalled train.
	Step 8	RD: Command drive/brake, release doors, sound the horn and inform passengers. Open/close doors by attendant (UC5.4-024).
	Step 9	RD: Check mission profile and proceed with manual speed control from remote with OAS in FS mode (ETCS).
Postcondition	Train drive until end of foreseen journey end or ATO is functional again.	
Use case notes	Basic paradigm is that Remote Driver just takes over failed functions of the automation system.	

UC5.4-036 Take responsibility of a GoA3 train with degraded ATO by remote driver

11.1.2 Take Responsibility Of A GoA4 Train In Degraded ATO Situation

This use case describes when the Remote Driver takes the control of a train in the degraded ATO GoA4 condition caused by a malfunctioning ATO component – all other components are functioning normally.

Use case field	Description
ID	UC5.4-037
Use case name	Take responsibility of a GoA4 train in degraded ATO situation
Main actor	Remote Driver

Other actors	Serviceable train (Train), IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Remote Driver (RD)	
Use case summary	The train is originally GoA4. The ATO is in fault and the Remote Driver takes the train responsibility (*1). This use case provides remote train control operation by a driver in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is to manage the ATO degraded condition by a Remote Driver. Minimize delays.	
Preconditions	Train is equipped with RTO components and full functional except ATO for GoA4 operation, e.g. all the perception sensors for driving remotely the train are working correctly. The train is registered at a remote supervision centre it reports to. The train is operative (e.g. UC5.4-012) and relies on a journey/mission (UC5.4-013). For instance, all internal tests have been performed. Either A) or B) is true: A) No driver monitors the train. The lost alarm policy redirects alarms to a RU-Supervisor responsible for the train. B) A Remote Driver is monitoring the train (e.g. UC5.4-014). Communication between the train and the control centre is working correctly. The train is in motion.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver. Delay can be minimized.
	Unsuccessful outcomes	The train cannot be remotely controlled. A driver must come to the train and take control of the train from the cabin.
Condition affecting termination outcome	**Outcome 2**	Communication failure and/or the train can drive with reduced speed.
Use case steps	**Step 1.0**	Train: 1. Detects the failure of automatic speed control function and change from AD to FS mode (ETCS). 2. Sends an alarm to the monitoring driver or the lost alarm policy, that needs to be acknowledged by the driver by taking control of the train. 3. Informs IM about the situation 4. starts coasting. The train applies full service-brake down to standstill and remains in Standstill 1. after at most T_MAX_UNPLANNED_TAKEOVER_TIME,

		2. if the train reaches T_TAKEOVER_MIN_SPEED, the train will apply service-brake down to standstill If A) is true (no monitoring driver), Branch to 1.1. If B) is true (driver already monitoring), Branch to 1.2. Note: the train moving on inertia is safe because ETCS still supervises speed and distance to SvL. Also, collision avoidance is still engaged. A conservative setting is T_MAX_UNPLANNED_TAKEOVER_TIME. In that case, the train immediately stops.
	Step 1.x.1	Train: if during step 1.0 to step 1.3, the train starts to apply service brake, it informs IOM that it starts this manoeuvre until some responsible can start it again.
	Step 1.x.2	Train: if during step 1.0 to Step 1.3, the train reaches standstill, it informs passengers about the situation and not to leave the train.
	Step 1.1	[A: no driver is monitoring. RUS receives the alarm (as defined by the lost alarm policy).] RUS: allocates a driver RD to the train. RUS acknowledges the alarm with options: A) Request to stop the train The train applies service-brake down to standstill. a. Request to continue coasting. Step1's timer for service brake application in less than T_MAX_UNPLANNED_TAKEOVER_TIME is reset, I.e. brake application is delayed by another T_MAX_UNPLANNED_TAKEOVER_TIME.
	Step 1.2	RD: starts monitoring the train. The train may be at standstill (Steps 1.0, 1.1), applying brakes or still be coasting.
	Step 1.3	RD: checks if the Perception sensors for driving the train work properly.
	Step 2.0	RD: Takes control of the train according to UC5.4-022. This acknowledges definitively the alarm in Step 1.0, i.e. the train will not apply service brake after T_MAX_UNPLANNED_TAKEOVER_TIME anymore.
	Step 2.x,1	If in step 1.x.1, IOM had been notified, it is notified that the train now has a driver in control.
	Step 2.x.2	If in step 1.x.2, passengers had been notified about the situation and not to leave the train, it is notified that the mission resumes, and thanked for its comprehension.
	Step 3	The driver now drives the train manually. It performs all actions foreseen in this context – see UC5.4-024
	Step 8	End of UC

Postcondition	ATO is not functional unless recovered. The train motion is protected according to the ETCS Signalling rules. Obstacle avoidance is engaged. On Failure, • The train remains stuck impeding traffic on the track. The Remote Driver may not be controlling it, or even monitoring it. • Other measures shall be taken to rescue the train: o An on-board driver is sent to the train to take control physically o Another train tows the train to a safe location On success, • The Remote Driver has the responsibility of the train. He/she continues the train's mission/journey manually until ATO is functional again or the train is withdrawn from service to be repaired. • This use case does not define if or when the train is withdrawn for service for reparation – this should be coordinated with RUS and IOM according to real conditions: o in a short delay, for instance before journey completion. In that case, a replacement train will take the passengers in charge o After journey completion o After completion of the train's service day
Use case notes	Basic paradigm is that the Remote Driver just takes over failed functions of the automation system. The train remains protected by the protections still functional.

UC5.4-037 Take responsibility of a GoA4 train in degraded ATO situation

11.2 DEGRADED PERCEPTION

11.2.1 Take Responsibility After Some Degraded Per In Goa4 Mode By Remote Control Driver

This use case describes when the Remote Driver takes the responsibility of the train in the degraded ATO GoA3 condition.

Use case field	Description
ID	UC5.4-038
Use case name	Take responsibility after some degraded PER in GoA4 mode by remote control driver
Main actor	Remote Driver RD
Other actors	Serviceable train (Train), APM/PER
Use case summary	This use case describes when the Remote Driver takes the responsibility of the train in the degraded ATO GoA3 condition. This use case provides remote train control operation by a driver in the control centre. The Remote Driver should be able to drive the train remotely as if on the train itself.
Applicability	Geographical: European level System level: RSC, Train

	Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is that a Remote Driver manages the degraded condition. Minimize delays.	
Preconditions	The train is equipped with RTO components and full functional except ATO for GoA4 operation, e.g. all the perception sensors for driving remotely the train are working correctly, all internal tests have been performed. The train is registered at some RSC it reports to The train is operative (e.g., UC5.4-012) and relies on a journey/mission (e.g., UC5.4-013). A Remote Driver is monitoring the train (e.g., UC5.4-014). Communication between the train and the control centre is working correctly. The train is moving in GoA4.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver and ready to move
	Unsuccessful outcomes	The train cannot be remotely controlled.
Condition affecting termination outcome	**Outcome 2**	Communication failure.
Use case steps	**Step 1**	Train: the train detects the failure of the PERception system. It applies a service brake intervention and sends an alarm to its responsible driver.
	Step 2	The driver receives an alarm: Due to some ATO GoA3 PERception fault the Remote Driver has to take the responsibility.
	Step 3	The Remote Driver checks that the Perception sensors for driving the train works properly. If yes Branch to Step 4 if not Branch to step 6
	Step 4	The Remote Driver takes control (push the button RSC-ClaimGrant on the driving workplace desk) and takes the full responsibility of the train by stepping through UC5.4-022.
	Step 5	The Remote Driver presses ATO-Engage on remote control desk for resuming the mission. Branch to step 7
	Step 6	The train cannot be remotely moved. A procedure for moving the train is necessary.
	Step 7	End of UC
Postcondition	The train is operative (e.g., UC5.4-012) and relies on a journey/mission (UC5.4-013). The driver is controlling the train. On success, if the sensors for moving the train work correctly, the Remote Driver can move the train in GoA2 or at traction & braking chain level according to the ETCS Signalling rules.	

	On failure, in case the sensors for moving the train didn't work the Remote Driver cannot move the train and a procedure to manage the train is necessary.
Use case notes	The procedure for moving the train is manage by the IM-

UC5.4-038 Take responsibility after some degraded PER in GoA4 mode by remote control driver

11.2.2 Take Responsibility After Some Degraded Perception In Goa4 Mode By Remote Control Driver

Use case field	Description	
ID	UC5.4-039	
Use case name	Take responsibility after some degraded PERception in GoA4 mode by remote control driver	
Main actor	On-board Automation System (OAS)	
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Remote Driver (RD)	
Use case summary	The Perception PER for GoA4 operation is in fault and the Remote Driver takes the train responsibility	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The main goal of this use case is that a Remote Driver manages the degraded condition, for instance successfully takes control of the train and drive it safely to the next stopping/rescue point. Minimize delays.	
Preconditions	The train is registered at some RSC it reports to "High availability of ETCS is mandatory for GoA3/4 operation (remote control is not possible if ETCS is in SF mode)." SRS 0.3.0 10.6 "(TCMS-12) GoA3/4 exported constraint: In remote control mode, TCMS shall act directly on traction or brakes (bypass of Train Protection or ADM commands)." SRS 0.3.0. 11.16.12 "(TUM-7.4) GoA3/4 exported constraint: Remote control shall be performed under ETCS supervision. Remote control shall not be possible when ETCS is in SF mode." SRS 0.3.0 12.18.7 "(TUM-8.1) GoA3/4 exported constraint: Remote control shall be performed through C48 with the support of a camera independent from PER module. Rationale: full coverage of GoA3/4 failure modes." SRS 0.3.0 12.18.8	
Termination outcome	**Successful outcomes**	Outcome 1: Train can continue without delay
	Unsuccessful outcomes	A driver must enter the train and takes control of the train
Condition affecting termination outcome	**Outcome 2**	Train can drive with reduced speed
Use case description	**Step 1**	OAS: Detect failure of perception function.

		According to the probability of collision with an obstacle associate to the track ahead of the train, OAS may decide 2.1 or 2.2. Step 4.x is performed in parallel of Step 2.x.
	Step 2.1.0	[Track ahead of train is a segregated track with probability of less than 10^{-7} 1/h and impact detection function is still available] OAS: Continue journey
	Step 2.1.1	OAS: Report failure to the failure of the perception function to trackside automation system TAS. While approaching the location for Step 2.1.2, Request for manual train control. Report that train is still running.
	Step 2.1.2	If the conditions for Step 2.1.0 are lost, Branch to Step 2.2.0 Branch to Step 3.1 otherwise.
	Step 2.2.0	[Otherwise] OAS: Apply brakes until train is at standstill and immobilize train with the cabin remaining virtually activated (if train is at open track with subject to obstacles).
	Step 2.2.1	OAS: Stop train in front of open track section.
	Step 2.2.2	OAS: Report stopping of the train and the failure of the perception function to trackside automation system TAS with the request for manual train control.
	Step 2.2.3	OAS: Inform passengers about the situation and not to leave the train.
	Step 2.2.4	TAS: Inform IM operations manager IOM and RUS about stopping and the failure of perception function.
	Step 3.1	RUS: Inform Remote Driver RD about the stalling or stalled train and request him to drive the train manually from remote.
	Step 3.2	RD: Takes control of the train – see UC5.4-022.
	Step 3.3	RD: Check mission profile and proceed with manual speed control from remote or with using automatic speed control.
Postcondition	Train moves at interstation in RTO.	
Use case notes	Basic paradigm is that Remote Driver just takes over failed functions of the automation system.	

UC5.4-039 Take responsibility after some degraded PERception in GoA4 mode by remote control driver

11.3 DEGRADED APM

11.3.1 Take Responsibility After Some Degraded Apm In Goa4 Mode By Remote Control Driver

Use case field	Description
ID	UC5.4-040
Use case name	Take responsibility after some degraded APM in GoA4 mode by remote control driver

Main actor	On-board Automation System (OAS)	
Other actors	IM Operations Manager (IOM), Railway Undertaking Supervisor (RUS), Remote Driver (RD)	
Use case summary	The Automatic Processing Module (APM) is in fault and the Remote Driver takes the train responsibility	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	Minimize delays.	
Preconditions	Train moves at interstation in GoA4. "High availability of ETCS is mandatory for GoA3/4 operation (remote control is not possible if ETCS is in SF mode)." SRS 0.3.0 10.6 "(TCMS-12) GoA3/4 exported constraint: In remote control mode, TCMS shall act directly on traction or brakes (bypass of Train Protection or ADM commands)." SRS 0.3.0. 11.16.12 "(TUM-7.4) GoA3/4 exported constraint: Remote control shall be performed under ETCS supervision. Remote control shall not be possible when ETCS is in SF mode." SRS 0.3.0 12.18.7	
Termination outcome	**Successful outcomes**	• Outcome 1: Train can drive without delay
	Unsuccessful outcomes	• A driver must enter the train and takes control of the train
Condition affecting termination outcome	**Outcome 2**	N/A
Use case description	**Step 1**	OAS: Detect failure of automatic processing function.
	Step 2	OAS: Apply brakes until standstill and immobilize train. The active cabin remains activated. Note: this contradicts definitions in X2Rail-4 v0.2, where PER maintains this state.
	Step 3	OAS: Report stopping of the train and the failure of the automatic processing function to trackside automation system TAS with the request for manual train control.
	Step 4	OAS: Inform passengers about the situation and not to leave the train.
	Step 5	TAS: Inform IM operations manager IOM and RUS about stopping and the failure.
	Step 6	RUS: Inform Remote Driver RD about the stalled train and request him to drive the train manually from remote.
	Step 7	RD: Confirm the request from OAS to take over control of the stalled train.
	Step 8	RD: Check mission profile. Note: with X2Rail-4 v0.2 definitions, train active cabin / direction of travel would have been lost in step 2 and

		would have to be redefined in step 8, for instance based on the train's movement authority or next stopping point.
	Step 9	~~RD:~~ with current definition of X2Rail-4 v0.2, RD would have to Activate remotely the appropriate cabin and enter train data and driver ID. With current definition this information step is avoided because the train direction of travel is not lost during the use case.
	Step 10	RD: Proceed with manual speed control from remote with OAS in FS mode (ETCS).
Postcondition	Train moves at interstation in RTO.	
Use case notes	Basic paradigm is that Remote Driver just takes over failed functions of the automation system.	

UC5.4-040 Take responsibility after some degraded APM in GoA4 mode by remote control driver

11.4 DEGRADED ATP

11.4.1 Take Responsibility In Degraded Etcs By Remote Control Driver

This use case describes when the Remote Driver takes the responsibility of the train in the degraded ETCS condition.

Use case field	Description
ID	UC5.4-041
Use case name	Take responsibility in degraded ETCS by remote control driver
Main actor	Remote Driver RD
Other actors	Serviceable train (Train), EVC, ATO
Use case summary	This use case provides remote train control operation by a driver in the control centre, with degraded on-board ETCS. The Remote Driver should be able to drive the train remotely as if on the train itself. Caution: this use-case foresees in step 6 the isolation of ETCS. This strongly degrades the safety of the train's motion. Current use-case is intended only as exceptional procedure e.g., to drive a stopped train to a rescue point and bring the complete system back to normal operations. Specific regulations should guarantee safety before step 6 is taken – see for instance step 4 and 5. See also R1 in Appendix 1, Refinements, p.157.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	The main goal of this use case is to manage the degraded condition from a Remote Driver.
Preconditions	The train is operative (e.g. UC5.4-012) and relies on a journey/mission (UC5.4-013). For instance, all internal tests have been performed. The train is registered at some RSC it reports to. A Remote Driver is monitoring the train (e.g. UC5.4-014). Communication between the train and the control centre is working correctly.

	At the start of the use-case, the train is still fully functional (autonomy capable).	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver and ready to move
	Unsuccessful outcomes	The train cannot be remotely controlled.
Condition affecting termination outcome	**Outcome 2**	Communication failure.
Use case steps	**Step 0.0**	Train: ETCS-OB becomes in fault. The train brakes until the standstill condition. The train delivers an alarm to its responsible driver.
	Step 1.0	RD: receives the alarm
	Step 2.0	RD: checks if the Perception sensors for driving the train works properly and visibility is given.
	Step 3.0	RD: takes control: pushes the button RSC-ClaimGrant on the Remote Driving desk, then steps through UC5.4-022.
	Step 3.1	RD: diagnoses that ETCS has to be isolated.
	Step 3.2	RD: checks in regulation book the train-related conditions allowing that ETCS is isolated. If not fulfilled, takes all action so that fulfilment is reached (visibility, service brake function, ...). At the end of this step, fulfilment is assumed reached. As if not, the train would have to be towed which is not covered in this use-case.
	Step 4.0	RD: requests IOM for the authorization to drive the train without ETCS supervision.
	Step 5.0	RD: The Remote Driver receives from the IM, the authorization to move the train without the supervision of the EVC ETCS on-board system
	Step 6.0	RD: isolates EVC ETCS on-board system This step is archived by the juridical recorder (see also section 3.9 p. 47)
	Step 7.0	RD: brings the train to the closest safe point to free the line, and allow the other trains to travel along the line.
	Step 8.0	End of UC
Postcondition	The train's ETCS is not functional. The driver is monitoring or controlling the train. On success: The driver controls the train, which is stopped at a safe point, the traffic is not impeded anymore. On Failure: The train is still at the same place as at use case start. Other recovery measures shall be taken, e.g.: • An on-board driver is sent to the train to recover it.	

	• Another train shall tow the failed train
Use case notes	The procedure is provided by the IM.

UC5.4-041 Take responsibility in degraded ETCS by remote control driver

11.4.2 Drive Remotely In Case Of Wayside Signalling System Failure

This use case describe how the Remote Driver takes the responsibility of the train due to a degraded wayside signalling system.

Use case field	Description	
ID	UC5.4-042	
Use case name	Drive remotely in case of wayside signalling system failure	
Main actor	Remote Driver	
Other actors	Serviceable train (Train), ETCS-OB, TAS, Infrastructure Operations Manager (IOM)	
Use case summary	This use case provides remote train control operation by a driver in the RSC. The Remote Driver should be able to drive the train remotely as if on the train itself.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The Remote Driver takes the responsibility of the train due to a degraded wayside signalling system	
Preconditions	Train is equipped with RTO components and full functional except ATO for GoA4 operation, e.g. all the perception sensors for driving remotely the train are working correctly, all internal tests have been performed. The train is registered at some RSC it reports to The train is operative (e.g. UC5.4-012) and relies on a journey/mission (UC5.4-013). For instance, all internal tests have been performed. A Remote Driver is monitoring the train (e.g. UC5.4-014). Communication between the train and the control centre is working correctly. The train is moving in GoA4.	
Termination outcome	**Successful outcomes**	The train is successfully controlled by a Remote Driver and ready to move
	Unsuccessful outcomes	The train cannot be remotely controlled.
Condition affecting termination outcome	**Outcome 2**	Communication failure.
Use case steps	**Step 1**	Train: Receives from RBC an emergency brake command. The train brakes until the standstill condition. The train delivers an alarm to its responsible driver.
	Step 2	RD: receives the alarm.

	Step 3	RD: checks if the Perception sensors for driving the train works properly.
	Step 4	RD: takes control: pushes the button RSC-ClaimGrant on the Remote Driving desk, then steps through UC5.4-022. The driver now is controlling the train.
	Step 5	RD: requests IOM for the authorization to driver the train without ETCS supervision.
	Step 6	Train: receives from TAS (RBC) the command to go in OS or SR.
	Step 7	RD: takes note about the command
	Step 8	RD: takes contact with IOM
	Step 9	IOM: delivers IOM the authorization to driver either in SR or in OS.
	Step 10	RD: switches ETCS in mode of his/her choice among SR and OS.
	Step 11	RD: brings the train to the closest safe point to free the line, and allow the other trains to travel along the line.
	Step 12	End of UC
Postcondition	The train's ETCS either in OS or in SR. The driver is monitoring or controlling the train. On success: The driver controls the train, which is stopped at a safe point, the traffic is not impeded anymore. On Failure: The train is still at the same place as at use case start. Other recovery measures shall be taken, e.g.: • An on-board driver is sent to the train to recover it. • Another train shall tow the failed train	
Use case notes	The procedure is provided by the IM.	

UC5.4-042 Drive remotely in case of wayside signalling system failure

12 DEGRADED MODES SPECIFIC TO REMOTE CONTROL

Following conditions introduce degraded modes specific to the remote control itself:

Bad weather and sensor limitations generate a poor visibility.

Even with good sensors, the visibility may be worse than expected (e.g., light conditions)

Degraded bandwidth forces to send to the remote driver's workplace some compressed video, also with loss of quality.

Latency in communication inserts a lag in displaying the train's environment to the remote driver.

Commands may reach the train too late or not.

Those conditions generate degraded modes that share common consequence:

- Degradation of video quality.
- Delayed video or sensors.
- Commands delayed or lost.

Ultimately, the remote driver may react too late to an obstacle on the track.

The above hazard is deemed SIL2.

Failing to react may impede safety-of-life (staff, trespasser at pedestrian hot-spots, animals, …) or allow damages to the train in the Sil2 domain (e.g. boogie due a collision with some artefacts left with offending intention, animals …).

The frequency of these events is high enough for the failure to react, even if conditioned by some bad weather or a communication link, to be inacceptable.

Hence operational behaviours of the train are defined that avoid hazard, while allowing operations as far as possible – graceful degradation principle.

- The train monitors the visibility distance and latency of the video stream delivered on the workplace.
- While visibility decreases and latency increases, the train decreases its maximum speed.
- If it drops below some ergonomics minima, the train intervenes e.g. with a service break intervention.

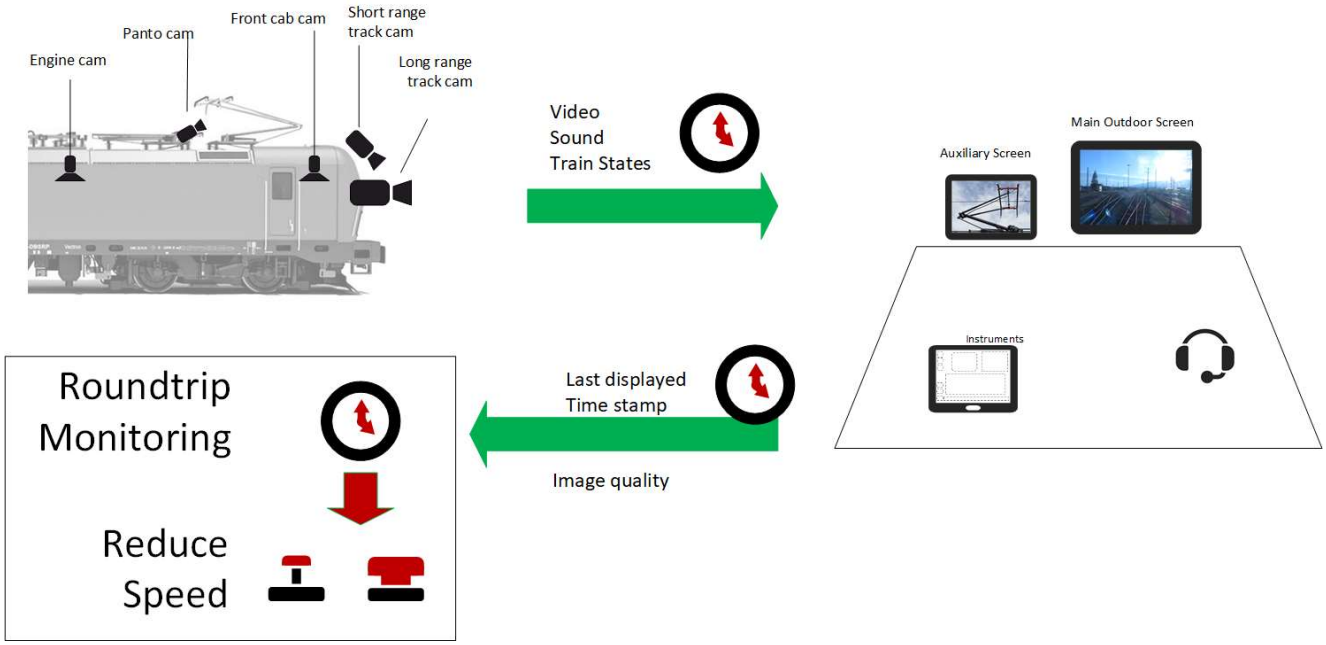

Figure 19: Train Monitoring of Remote Driver workplace

12.1 ASUMPTIONS

In this section, definitions are taken that permit to precise the proposed behaviour. It shall be refined in WP6 task 6.7's human factor analysis and task 6.8 architectural considerations. Parameters are defined that intend to test/refine the degree of freedom fit for each train.

12.1.1 Video Latency

Experience with drone pilots shows that

- A latency of 100 ms between pilot command and confirmation of execution is unnoticed by the human. From this point on, the ergonomics energy he/she needs to maintain piloting is measurable by observers.
- With a latency of 200 ms, the pilot is aware that he/she needs to invest some additional energy to pilot. This awareness is a light discomfort.
- With a latency in reaction time between reality and video > 500 ms, pilots need to dedicate such an amount of their cognitive energy that their performance tasks other than controlling vehicle attitude have drastically dropped already – plan mission, 'listen to' external environment.

Furthermore, if latencies grow, reaction distance become excessively long compared to the agility of movement of human obstacles:

		Driven distance (m)									
Train speed (km/h)	360	10	20	30	40	50	60	70	80	90	100
	250	6,94	13,89	20,83	27,78	34,72	41,67	48,61	55,56	62,5	69,44
	160	4,44	8,89	13,33	17,78	22,22	26,67	31,11	35,56	40	44,44
	100	2,78	5,56	8,33	11,11	13,89	16,67	19,44	22,22	25	27,78
	50	1,39	2,78	4,17	5,56	6,94	8,33	9,72	11,11	12,5	13,89
	30	0,83	1,67	2,5	3,33	4,17	5	5,83	6,67	7,5	8,33
	10	0,28	0,56	0,83	1,11	1,39	1,67	1,94	2,22	2,5	2,78
	5	0,14	0,28	0,42	0,56	0,69	0,83	0,97	1,11	1,25	1,39
	4	0,11	0,22	0,33	0,44	0,56	0,67	0,78	0,89	1	1,11
	3	0,08	0,17	0,25	0,33	0,42	0,5	0,58	0,67	0,75	0,83
	2	0,06	0,11	0,17	0,22	0,28	0,33	0,39	0,44	0,5	0,56
	1	0,03	0,06	0,08	0,11	0,14	0,17	0,19	0,22	0,25	0,28
		0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
		time (s)									

Table 8: Distance driven by train during video latency, function of speed

To consider those 2 phenomena, a maximum speed $V_{MAX\_VIDEO\_LATENCY}$ is defined for a train remotely controlled, $V_{MAX\_VIDEO\_LATENCY} = f(T_{LATENCY})$, as shown in Figure 20 p.144.

$V_{MAX\ TRAIN}$ and $V_{MIN\ AUTO}$ are properties of the train:

$V_{MAX\ TRAIN}$: Maximum speed for which the train is accredited.

$V_{MIN\ AUTO}$: Minimum speed that can be controlled/automated by the train

Following parameters are defined by ergonomics consideration:

T_{LAT_NORMAL} is defined as the highest latency without acceptable influence on the driver's performance.

T_{LAT_CRITIC} is the last latency reasonably requirable from a driver in operations

$V_{LAT\_CRITIC\_OPS}$ is its associated maximum speed in operations.

Below T_{LAT_NORMAL}, the train's maximal speed remains $V_{MAX\ TRAIN}$. From T_{LAT_NORMAL} to T_{LAT_CRITIC}, the train's maximum speed decreases linearly with the video latency $T_{Latency}$. The intend is that the lowered speed releases some of the increase ergonomic energy required by the increases $T_{Latency}$., while still enabling the maximum reasonable service.

From TLat_Critic on, the discomfort due to the increased TLatency is considered too high to enable normal operations. The allowed speed drops, not yet to 0 though.

To avoid leaving a train in place due to some this latency, supposing that image quality is good, an 'unsustainable load' driving mode is defined. This mode must be acknowledged by the driver. In this mode, reaction times are considered so long that the agility of human obstacles will lead them to appear on the video stream too late.

$V_{LAT\_CRITIC\_LASTCALL}$ is calibrated so low that the human obstacles themselves are unlikely to be surprised by the train.

The driver's tasks shall be reduced to an absolute minimum: only monitoring the train's motion. Any other responsibility shall be moved to colleagues.

The train's maximum speed continues to decrease while the latency increases until the train cannot automate a lower speed anymore.

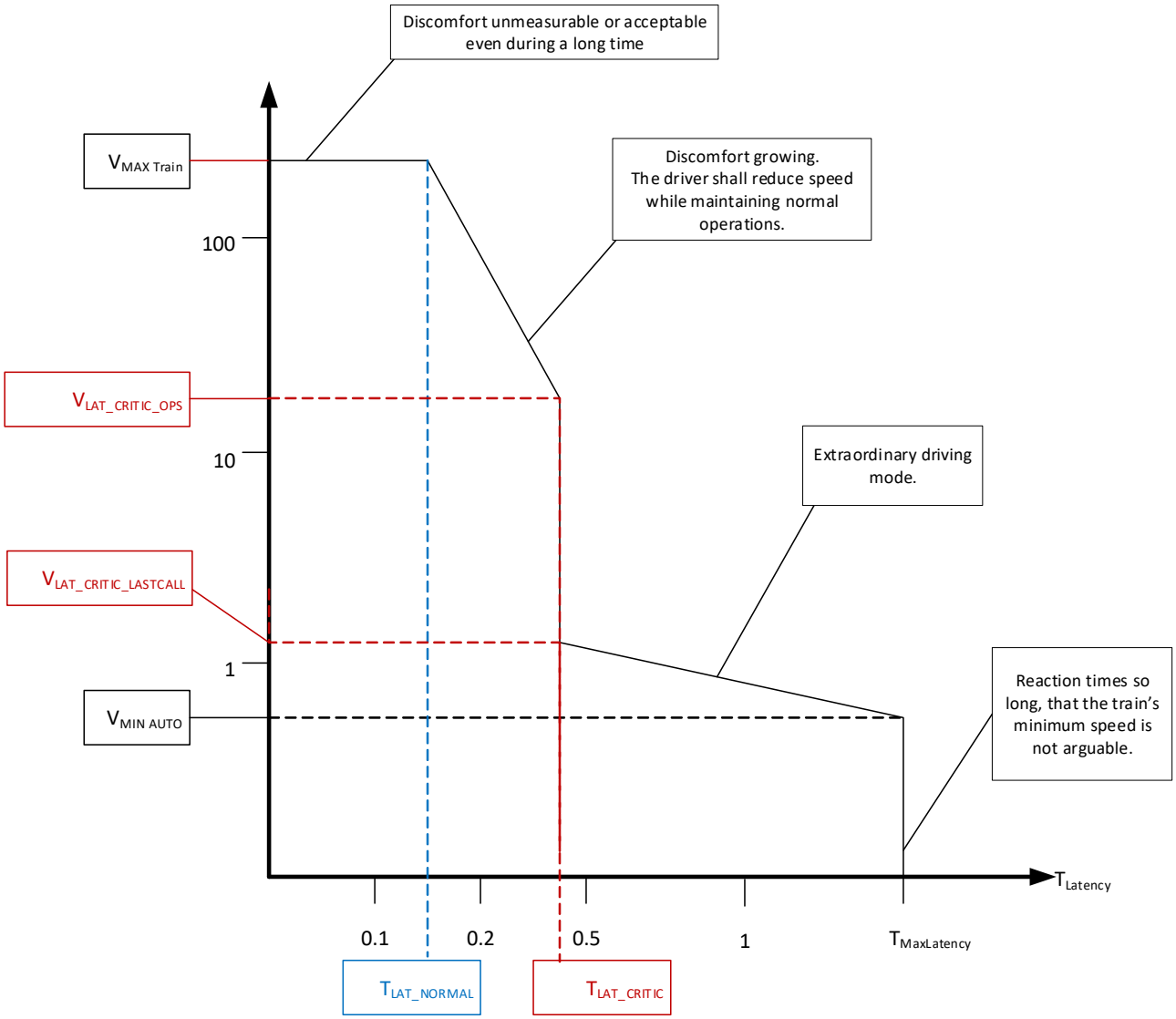

Figure 20: Maximum speed function of video latency

12.1.2 Command latency

The driver is given an interface allowing him / her to enter his / her commands to the train (Traction, Brake, Engage ATO).

The HMI Design assumes that those commands are executed with a maximum time $T_{REMOTE\_CMD\_BUDGET}$. This budget specifies a time, from the moment the command is issued, after which the command is not valid anymore.

After a train has implemented a command, its takes $T_{REMOTE\_CMD\_BUDGET}$ as its new reference. When time passes without implementing (receiving or managing to implement) new commands, the train builds up T_{REMOTE_BUDGET} = $T_{REMOTE\_CMD\_BUDGET}$ + Time Elapsed since Sending of the command determining current reference $T_{REMOTE\_CMD\_BUDGET}$.

If current time T_{NOW} > T_{REMOTE_BUDGET}, i.e. the last implemented command has grown too old, the train implements a braking intervention. Note that this case should happen rarely as new commands constantly replace the old one, thus refresh the budget.

The train remains waiting for a reconnection with acceptable latencies, or take-over by an on-board driver.

12.1.3 Bad visibility: weather and video codecs

In general, the driver is today already capable to define his/her reasonable maximum speed according to visibility. This intelligent decision capability remains for remote control.

Remote control reinforces the visibility constraint. Therefore, the driver may additionally be given an interface allowing him / her to enter his / her visibility distance in meter, $D_{MAX\_VISIBILITY\_HMI}$. As this distance is set by the driver him/herself, it is considered encompassing visibility degradation due to both bad weather and video compression due to bandwidth bottlenecks.

Optionally, $D_{MAX\_VISIBILITY\_WEATHER}$ may be estimated by the perception system as the maximum visibility due to weather. $D_{MAX\_VISIBILITY\_COMPRESSION}$ may also be estimated based on codec compression. These features are envisioned as comfort features and are conditioned by thorough human factor analyses.

Considering $D_{OVERALL\_VISIBILITY}$, the maximum visibility given by the complete chain: sensors on the train, codecs, screens on the remote workplace,

$E_{MAX\_VISIBILITY\_COMPRESSION} = D_{MAX\_VISIBILITY\_COMPRESSION} / D_{OVERALL\_VISIBILITY}$

$E_{MAX\_VISIBILITY\_WEATHER} = D_{MAX\_VISIBILITY\_WEATHER} / D_{OVERALL\_VISIBILITY}$

If not estimated, $E_{MAX\_VISIBILITY\_WEATHER} = E_{MAX\_VISIBILITY\_COMPRESSION} = 1$.

$D_{MAX\_VISIBILITY\_ESTIMATED} = D_{OVERALL\_VISIBILITY} * E_{MAX\_VISIBILITY\_COMPRESSION} * E_{MAX\_VISIBILITY\_WEATHER}$

$D_{MAX\_VISIBILITY\_ESTIMATED} = D_{MAX\_VISIBILITY\_WEATHER} * E_{MAX\_VISIBILITY\_COMPRESSION}$

Considering $D_{MAX\_VISIBILITY} = \min(D_{MAX\_VISIBILITY\_HMI} , D_{MAX\_VISIBILITY\_ESTIMATED})$,

$V_{MAX\_VISIBILITY}$ is deduced of $D_{MAX\_VISIBILITY}$ the same way ETCS's level crossing speed restriction (LX SR) is calculated.

This speed is then enforced by the train itself: in pedestrian hot spots – level-crossings, platforms, areas in which a temporary speed limit is defined.

12.2 USE CASES

12.2.1 Drive Remotely With A Poor Visibility Due To Weather

Use case field	Description
ID	UC5.4-043
Use case name	Drive remotely with a poor visibility due to weather
Main actor	Remote Driver
Other actors	Serviceable train (Train)
Use case summary	The visibility provided to a Remote Driver is not as good as expected. This use case drafts a strategy to avoid hazardous motions, while providing availability.

Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The train offers maximum drivability without posing any hazard to its environment, although visibility is bad.	
Preconditions	The train is controlled by a Remote Driver. As an option, the train is equipped so that it can estimate the train's visibility. The maximum speed of the train is V_{MAX_TRAIN}, when visibility is optimal. Note: No reduction of visibility due to a bad connection is considered in this scenario, I.e. $E_{MAX\_VISIBILITY\_COMPRESSION}$=1.	
Termination outcome	**Successful outcomes**	The train's $D_{MAX\_VISIBILITY}$ has been updated. The associated maximum speed is enforced.
	Unsuccessful outcomes	The maximum speed associated to the degraded visibility is not enforced.
Condition affecting termination outcome	**Outcome 2**	Perception available.
Use case description	**Step 1**	The weather conditions get worse. The train detects this degradation.
	Step 1.1	The train computes $D_{MAX\_VISIBILITY\_WEATHER}$. It updates $D_{MAX\_VISIBILITY\_ESTIMATED}$, $D_{MAX\_VISIBILITY}$ and $V_{MAX\_VISIBILITY}$ accordingly (see definitions). The train updates the maximum permitted speed to $V_{MAX\_VISIBILITY}$.
	Step 1.2	The remote operations HMI displays to the driver his/her current maximum speed, and that the reason for this is the bad visibility.
	Step 2.0	The train is still too fast. The RDR decides to reduce the speed further. He / she opens a visibility dialog in the HMI. He / she is presented with both $D_{MAX\_VISIBILITY\_ESTIMATED}$ and $V_{MAX\_VISIBILITY}$ as the train's recommendation. He / she can reduce the speed by: • Entering a $D_{MAX\_VISIBILITY\_HMI}$ as some reduction of $D_{MAX\_VISIBILITY\_ESTIMATED}$. • Reducing $V_{MAX\_VISIBILITY}$. $D_{MAX\_VISIBILITY\_HMI}$ is automatically updated accordingly. $D_{MAX\_VISIBILITY}$ and $V_{MAX\_VISIBILITY}$ are automatically recalculated, according to the rules defined for ETCS's LX Speed.

		Once satisfied with a new set of $D_{MAX\_VISIBILITY}$ and $V_{MAX\_VISIBILITY}$, he / she validates this choice. According to its current speed and the new $V_{MAX\_VISIBILITY}$, the train computes an estimated slow-down time T_SLOW_DOWN necessary to reach $V_{MAX\_VISIBILITY}$. Note: the driver could also increase current $D_{MAX\_VISIBILITY\_HMI}$ and $V_{MAX\_VISIBILITY\_HMI}$. In case they are increased so that $D_{MAX\_VISIBILITY\_HMI}$ >= $D_{MAX\_VISIBILITY\_WEATHER}$, $D_{MAX\_VISIBILITY}$ is defined by $D_{MAX\_VISIBILITY\_WEATHER}$ only. In the future, both Steps 3.0 and 4.0 are implemented in parallel.
	Step 3.0	If driving automatically above the new $V_{MAX\_VISIBILITY}$, the train slows down to this the new $V_{MAX\_VISIBILITY}$. If driving manually, the Remote Driver slows down to this new this new $V_{MAX\_VISIBILITY}$.
	Step 4.0	After T_SLOW_DOWN since validation of $V_{MAX\_VISIBILITY}$ in step 2.0, the train monitors $V_{MAX\_VISIBILITY}$. In case it exceeds it, it implements a braking intervention.
Postcondition	$D_{MAX\_VISIBILITY}$ and $V_{MAX\_VISIBILITY}$	
Use case notes	-	

UC5.4-043 Drive remotely with a poor visibility due to weather

12.2.2 Drive Remotely With A Poor Up-Link Connection

Use case field	Description
ID	UC5.4-044
Use case name	Drive remotely with a poor up-link connection
Main actor	Train
Other actors	Serviceable train (Train), Remote Supervision Centre (RSC)
Use case summary	The quality of connection between train and Remote Supervision CentreSC does not allow an optimal transmission of video and sound to the Remote Driver.
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles
Main goal	The purpose of this use case is to specify some graceful degradation of the train's motion speed while the quality of the communication sinks and degrades the quality of the video proposed to the Remote Driver. - Images are delayed - The frequency of images decreases - The image quality decreases

Preconditions	A Remote Driver drives the train, either automatically (ATO) or manually (traction/braking). At scenario start, the quality of the video is maximal: $T_{LATENCY}$ <= $T_{LATENCY\_CRITIC}$ and $D_{MAX\_VISIBILITY\_COMPRESSION}$ = $D_{MAX_VISIBILITY}$_NOMINAL. <u>Remaining all along the scenario:</u> No reduction of visibility due to the weather is considered in current scenario. For this, current scenario needs to be combined with UC5.4-043. It is not assisted by PER for obstacle avoidance, hence collision with pedestrians has to be considered as consequence of objects unseen by the driver. The Train's ATP is assumed up, running and functional. SIL4 hazards (collision with other trains, derailment while driving over unlocked blades) are excluded. A technical assumption is taken along this scenario: The train regularly receives a report about the age $T_{LATENCY}$ of the last image (frame) the workplace has received in the train's video flow about its environment. Attached to it, it gets a report about $D_{MAX\_VISIBILITY\_COMPRESSION}$ displayed by the workplace.	
Termination outcome	**Successful outcomes**	The Remote Driver continues driving the train. The train monitors its speed and enforces a safely reduced maximum speed.
	Unsuccessful outcomes	The train generates an accident or It stops while it could be driven safely at reduced speed.
Condition affecting termination outcome	**Outcome 2**	How degraded the connection defines the outcome of this use case.
Use case description	**Step 1**	The quality of the connection supporting the video stream between train and remote supervision centre goes down. The Remote Driver's workplace detects it and reports to the train. Notes:1) This step is inserted to give a direction to the 'story' in this use cases. The use case could have been done with a connection getting better. 2) Monitoring of network quality and adaption of codec compression or frame frequency is a feature provided by off-the-shelves IP layers and codecs. To prepare later COTS-enabling safety concepts, this use case documents this step 1.x. It is not, however, strictly operational. The use case could start with next
	Step 1.1	As a consequence, the train starts reducing the image frequency and video quality of the stream it sends to the workplace ($E_{MAX\_VISIBILITY\_COMPRESSION}$<1).
	Step 1.3	The workplace collects the video quality $E_{MAX\_VISIBILITY\_COMPRESSION}$ and measures the latency of the video it receives TLATENCY.
	Step 2	The workplace reports $E_{MAX\_VISIBILITY\_COMPRESSION}$ and TLATENCY to the train. Note: as this use case is intended to address a hazard – train driving inside MA without obstacle management (automatic or by driver), from now on, all steps are considered safety relevant (SIL 4 being still addressed by the train's ATP).

	Step 3.0	The train receives $E_{MAX\_VISIBILITY\_COMPRESSION}$ and TLATENCY as occurred at the workplace. They replace its former perception of it.
	Step 3.1	At any time since the last reception of TLATENCY, the train considers the TLATENCY_ASSUMED on the HMI as TLATENCY + TSINCE_RECEPTION_OF_TLATENCY as occurred at the workplace. Jump in parallel to step 5.x and 6.x to assess $E_{MAX\_VISIBILITY\_COMPRESSION}$ and TLATENCY_ASSUMED.
	Step 5 .1	The train considers the new MAX_VISIBILITY_COMPRESSION in its estimation of $D_{MAX_VISIBILITY}$_ESTIMATE = $E_{MAX\_VISIBILITY\_COMPRESSION} * D_{MAX\_VISIBILITY\_WEATHER}$.
	Step 5 .2	The train updates $D_{MAX\_VISIBILITY}$ = min($D_{MAX\_VISIBILITY\_HMI}$, $D_{MAX\_VISIBILITY\_ESTIMATED}$)
	Step 6.0	The train monitors $V_{MAX\_VISIBILITY}$ = f ($D_{MAX\_VISIBILITY}$).
	Step 6.1	The train computes V_MAX_LATENCY = f (TLATENCY_HMI) according to the definitions in 12.1.1, Video Latency, p.142.
	Step 6.2	The train monitors V_MAX_LATENCY: if the train exceeds it, brakes until V_TRAIN < V_MAX_LATENCY. If TLATENCY_HMI > TLAT_CRITIC, jump to Step 5.3. Jump to Step 7 otherwise.
	Step 6.3	If TLATENCY_HMI > TLAT_CRITIC, the train sends an alarm to the driver. If the driver does not confirm this alarm in T_CRITICAL_VIDEO_LATENCY_ALARM_ACKNOWLEDGEMENT, the train brakes in emergency until it stops. The use case ends. If the driver confirms this alarm, the use case continues in Step 6.4.
	Step 6.4	The Remote Driver drives in 'unsustainable load' mode. After T_EXTRAODINARY_MODE_ALARM_PERIOD, jump back to Step 6.3.
	Step 7	The Remote Driver drivers in 'Unmeasurable discomfort' or 'Growing Discomfort' mode.
Postcondition	The train drives in 'Unmeasurable discomfort', 'Growing Discomfort', or 'unsustainable load' mode. 'Unsustainable load' requires periodic alarm acknowledgement. As steps 2-7 are performed periodically, those modes change swiftly. Options: the Train may set a maximum duration of 'duration*latency' for a single driver. After this budget is elapsed, the driver shall have a ½ hour break. To provide continuity of service, he/she may be replaced by another Remote Driver. Some fatigue detection may also be enforced while the driver is in 'unsustainable load'.	
Use case notes	Covers NS-HRN-3, Monitor connection quality, NS-HRN-5, Handle loss of remote connection, NS-HRN-4, Handle poor remote connection quality, ADIF-25, Loss of communication with the automatic train.	

UC5.4-044 Drive remotely with a poor up-link connection

12.2.3 Drive Remotely And Loose Track Sensors

Use case field	Description	
ID	UC5.4-045	
Use case name	Drive remotely and loose track sensors	
Main actor	Serviceable train (Train)	
Other actors	Remote Driver (RD), Infrastructure Operations Manager (IOM), Railway Undertaking Supervisor (RUS)	
Use case summary	This use case happens during remote train control operation by a driver in the control centre. At least one perception sensor (camera) doesn't work properly.	
Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The purpose of this use case is to specify train and driver behaviour when the track sensors supporting the remote control are lost.	
Preconditions	A Remote Driver drives the train, either automatically (ATO) or by hand (traction/braking). At scenario start, track sensors supporting the remote control (mainly video) are functional. <u>Remaining all along the scenario:</u> It is not assisted by PER for obstacle avoidance, hence collision with pedestrians has to be considered as consequence of objects unseen by the driver. The Train's ATP is assumed up, running and functional. SIL4 hazards (collision with other trains, derailment while driving over unlocked blades) are excluded. A technical assumption is taken along this scenario: The train regularly receives a report about the age $T_{LATENCY}$ of the last image (frame) the workplace has received in the train's video flow about its environment.	
Termination outcome	**Successful outcomes**	The train has stopped. Collisions with obstacles are avoided.
	Unsuccessful outcomes	The train continues driving. Collisions with obstacles are possible.
Condition affecting termination outcome	**Outcome 2**	-
Use case description	**Step 1**	Train: The track sensors are fully functional.
	Step 1.1	Train: The track sensors fail. 2 possible kinds of failure: a) The train detects the failure and can diagnose that further operations would be dangerous. Branch to step 3.1 b) The train cannot detect the failure. Branch to Step 2

	Step 2	[The train detects its sensor failure] The train implements a full service-brake intervention. It sends a diagnostic to the driver, IOM and RUS. Once at standstill, it activates the stationary brake. Branch to Step 5
	Step 3 .1	[The train has not detected the sensor failure] Driver: The workplace continues to display the video flow it receives – for instance black, or with lines in the image. The driver observes it.
	Step 3.4	RD: the driver detects that the quality of the video he/she observers is too poor for operations. He/she brakes down to standstill and activates the stationary brakes.
	Step 4	RD: coordinates with IOM and RUS so an on-board driver is sent to the train and the mission can be continued.
Postcondition	The train drives in 'Unmeasurable discomfort', 'Growing Discomfort', or 'unsustainable load' mode. 'Unsustainable load' requires periodic alarm acknowledgement. As steps 2-7 are performed periodically, those modes change swiftly. Options: The Train may set a maximum duration of 'duration*latency' for a single driver. After this budget is elapsed, the driver shall have a ½ hour break. To provide continuity of service, he/she may be replaced by another Remote Driver. Some fatigue detection may also be enforced while the driver is in 'unsustainable load'.	
Use case notes	Covers NS-HRN-3, Monitor connection quality, NS-HRN-5, Handle loss of remote connection, NS-HRN-4, Handle poor remote connection quality, ADIF-25, Loss of communication with the automatic train.	

UC5.4-045 Drive remotely and loose track sensors

12.2.4 Drive Remotely With A Poor Down-Link Connection

Use case field	Description
ID	UC5.4-046
Use case name	Drive remotely with a poor down-link connection
Main actor	Serviceable train (Train)
Other actors	Remote Driver, its HMI in the Remote Supervision Centre (RSC)
Use case summary	The quality of connection between train and RSC does not allow an optimal transmission of commands to the train. The use case does not address the fact that a command cannot be executed as such because the component executing it is defect. Analysis of degrade mode is another scope. This use case covers only delay in the flow of command and their execution.

Applicability	Geographical: European level System level: RSC, Train Operational category: passenger, freight, urban, regional, mainline and inspection vehicles	
Main goal	The purpose of this use case is to specify some safe behaviour for the train when the commands coming from the remote operations HMI do not flow down to the train anymore.	
Preconditions	A Remote Driver drives the train, either automatically (ATO) or by hand (traction/braking).	
Termination outcome	**Successful outcomes**	The train has stopped – accidents are avoided.
	Unsuccessful outcomes	The train drives wildly, which could generate an accident.
Condition affecting termination outcome	**Outcome 2**	How degraded the connection defines the outcome of this use case.
Use case description	**Step 1**	The quality of the connection supporting the commands between remote supervision centre and train goes down.
	Step 2	The workplace stamps every command to the traction chain or ATO with $T_{REMOTE\_CMD\_BUDGET}$. Note: as this use case is intended to address a hazard – train driving inside MA independently of driver, or against its will (automatic or by driver), from now on, all steps are considered safety relevant, SIL 4 being still addressed by the train's ATP. Should the train violate the location supervised by its ATP, please Branch to 6.1. Should it violate the speed supervised by the ATP, please jump to 6.2.
	Step 3	The train receives a command with $T_{REMOTE\_CMD\_BUDGET}$. It replaces its former perception of it.
	Step 4	At any time since the last reception of $T_{REMOTE\_CMD\_BUDGET}$, the train considers the TCMD_BESTBEFORE as $T_{REMOTE\_CMD\_BUDGET}$ - TSINCE_CMD_WAS_INPUT_ON_HMI.
	Step 5	If current time T_NOM > TCMD_BESTBEFORE, the train stops. Branch to step 7
	Step 6.1	[Distance supervision to the location supervised by its ATP shows that it is about to violate it] Train: the train trips (emergency braking interventions
	Step 6.2	[The train violates the speed supervised by its ATP]

		Train: the train trips (emergency braking interventions)
	Step 7	Use case ends
Postcondition	The train drives with a command execution latency acceptable, or it is stopped.	
Use case notes	Covers NS-HRN-3, Monitor connection quality, NS-HRN-5, Handle loss of remote connection, NS-HRN-4, Handle poor remote connection quality, ADIF-25, Loss of communication with the automatic train. See also section 12.1.1. about Video Latency.	

UC5.4-046 Drive remotely with a poor down-link connection

13 CONCLUSIONS

The fundamental step in defining areas of interest for the development of Remote Driving systems is a difficult objective. The task 5.4 result attempts to provide the required detail and clarity on these areas of interest.

Due to the collaboration of partners ranging from operators, infrastructure managers, industrial suppliers and research groups, the final result brings the culmination of the results developed over the last nine months through their expertise. The definition of use cases, operational parameters and scenarios for Remote Driving systems will constitute an important input for the work-packages following task 5.4 and will offer the right operational scenarios to focus on for further developments.

Unfortunately, the expected contribution from SP and other FPs did not arrive as initially expected. However, this did not stop the activities which were carried out until completion. All the objectives foreseen in [GA] for task 5.4 were carried out within the scheduled time and this represents an excellent result considering that the group of partners also had to align on the meaning of operation aspects associated with Remote Driving reported in section 2.5. Once this initial obstacle was overcome, all the partners produced their contribution by creating this document.

Compared to what was achieved in the X2Rail-4's and TAURO projects, a notable step forward has certainly been made, defining a complete set of use cases for Remote Driving. To achieve this result, all operational aspects were analysed.

The set of use cases and the definition of the changes in the logical states constitutes a valid basis for the creation of the architecture and the drafting of the functional requirements. The foundations were also created for the creation of test cases to verify the functioning of future prototypes.

For the sake of completeness, not all areas have been explored with the same level of depth because the level of knowledge of the partners involved does not always cover every detail. For example, the part concerning the aspects related to the needs of freight trains was not explored in depth because the skills of the partners involved in task 5.4 were more aimed at solutions for passenger trains. The scope of the Remote Driver for freight trains has been addressed but not in the same detail as that for passenger trains. In the FP5 project all areas of the FDFTO are covered. In the future there should be an alignment activity between the two projects (FP2 and FP5) to have aligned solutions.

This deliverable will be shared with the System Pillar so that it can consider this as input to the definition activities of the part relating to the Remote Driver.

Furthermore, D5.4 is an input for the continuation of activities in R2DATO for tasks 6.7 first and then 6.8 of WP6.

- From the [GA] for task 6.7 "Based on the use cases and operational parameters defined in WP5, a set of functional and non-functional requirements will be specified."
- From the [GA] for task 6.8 "The main goal of this task is to review the architecture for the “Remote Driving and command” subsystem developed in TAURO and might be amended after considering the requirements from SP (System requirements), and output from Task 6.7 in order to address the set of new use cases identified in the Task 5.4."

APPENDIX 1: DESCOPED OR DELETED USE CASES, REFINEMENTS

While current work went on, some use cases were identified as potentially relevant for operations, but not processed. Some use cases were merged during TMT review in new use case UC5.4-047. Lastly some variants of the process were pointed during the review. The use-case were not changed. They may though influence the requirements in WP6 task 6.7.

13.1 DESCOPED USE CASES

13.1.1 Monitoring Without Emergency Braking Capacity

This ergonomic state may be necessary if a user without driving skills is asked to monitor a train. The idea is to avoid spurious braking with high impact on operations. The RU-Supervisor was envisioned. Observers during test sessions may also be candidates. However, restraining the emergency braking capability seemed a breech in safety principles that needed more experience before decision.

13.1.2 Processes Associated With The Instruments Screen

In Figure 6: Remote Operations HMI, p.35, an instruments screen permits to show detailed, train specific, components of the train. This screen is provided for both on-board and remote workplaces. A typical application is diagnostic. This screen corresponds to an existing state of the art in today cabs but depends on the rolling stock structure itself. Specifying in a standardised way would require either an effort in harmonization far beyond task 5.2, or standards about remote displays yet to be defined.

Therefore, although this screen is replicated for the remote cabin as ‘expected maintenance screen’ according to today’s state of the art already, the use cases associated to it were delayed until more experience could be gathered.

13.1.3 Emergency braking while monitoring several trains

While monitoring several trains, a driver shall pick-up the train of its interest before pushing the emergency brake. However, in the hurry, he/she may forget. Several ergonomics are envisioned for this case:

1. All trains implement an emergency braking intervention. This strategy, by essence safe, may have tremendous impact on operations.
2. The driver’s HMI requests the driver which train is meant. No train brakes until the driver answers. This strategy seems to the authors of the document not acceptable from the point of view of safety.

a combination of both:

3. The driver’s HMI requests the driver which train is meant. If no answer is given in less than a fixed duration, all trains implement the EBI.

Compared to 1), 3) is more operations-friendly, at some cost to the safe reaction. The authors of this document lack real operations experience to assess how far the time lost at the beginning of 3) makes it unacceptable (safety) toward 1).

As first demonstrators will unlikely implement multi-train monitoring, this decision is delayed until more experience could be gathered. 1) is the temporary recommendation, unless 3) is currently under test.

13.1.4 Managing fire on board

During review, a use-case related to the isolation of power sources in fault was proposed. Unfortunately, redactional cut had already been done / time was missing to consider all aspects of fire management procedures.

This use-case may be generated easier once WP6.8 permits to benefit from the design foundations laid for [D5.1] use-cases UC5.1-036, UC5.1-055 and UC5.1-056.

- UC5.1-036, Fire onboard locomotive or empty passenger train. The detection of fire, i.e., the trigger of this use case can be: Onboard device detection, Trackside device detection
- UC5.1-055, Handle fire accident on passenger train - in station (at standstill) - detected by train unit (e.g. PER / CCTV on-board). This use case can be triggered not only by the detection from train unit, but also possible from trackside unit or people (railway staff, passengers or travellers).
- UC5.1-056, Handle fire accident on passenger train - running, this use case can be triggered not only by the detection from train unit, but also possible from trackside unit or people (railway staff, passengers or travelers).

DELETED USE-CASES

This section documents use-cases deleted after release 01.

Use case field	Description	
ID	UC5.4-002	
Use case name	Obsolete: merged into UC5.4-047 in edition 04	
Use case notes	**Traceability**	See points Alstom.Findings.9-13, .15 in FP2-T5_4-T-MER-027-01.

UC5.4-002 Obsolete: merged into UC5.4-047 in edition 04

Use case field	Description	
ID	UC5.4-003	
Use case name	Obsolete: merged into UC5.4-047 in edition 04	
Use case notes	**Traceability**	See points Alstom.Findings.9-13, .15 in FP2-T5_4-T-MER-027-01.

UC5.4-003 Obsolete: merged into UC5.4-047 in edition 04

Use case field	Description
ID	UC5.4-004
Use case name	Obsolete: merged into UC5.4-047 in edition 04

Use case notes	Traceability	See points Alstom.Findings.9-13, .15 in FP2-T5_4-T-MER-027-01.

UC5.4-004 Obsolete: merged into UC5.4-047 in edition 04

Use case field	Description	
ID	UC5.4-005	
Use case name	Obsolete: merged into UC5.4-047 in edition 04	
Use case notes	Traceability	See points Alstom.Findings.9-13, .15 in FP2-T5_4-T-MER-027-01.

UC5.4-005 Obsolete: merged into UC5.4-047 in edition 04

Use case field	Description	
ID	UC5.4-006	
Use case name	Obsolete: merged into UC5.4-047 in edition 04	
Use case notes	Traceability	See points Alstom.Findings.9-13, .15 in FP2-T5_4-T-MER-027-01.

UC5.4-006 Obsolete: merged into UC5.4-047 in edition 04

REFINEMENTS

The authors choose to provide concrete use-cases, including detailed operational assumptions, for instance also including some ergonomic proposals. These contents are proposed as an anticipation of tasks 6.7 and 6.8.

Task 6.7, Set of non-functional and functional requirements for remote driving (incl. human factors)

Task 6.8, Definition of architecture and interfaces for remote driving in passenger/ freight/ inspection vehicles and tramways.

Some reviewers pointed out aspects, details or principles. They have made some alternative proposal. A consensus could not be found in the short review time. The current section collects those arguments for them to nurture the works of the above.

R1: Remote control without ATP may be impossible

According to feedbacks [REV 01] 100 and 112, performing UC5.4-041, a remote driver taking responsibility in degraded ETCS, may not be desirable or possible. Safety concerns were issued. X2Rail Requirements were quoted:

> *7.10.1.1.1 The remote driving is used in GoA3/4 to manage some degraded situations where the train is still able to move under ETCS supervision. The train is stopped after a failure of GoA3/4 system and there is no driver available to permit a switch to GoA0, GoA1 or GoA2.*
>
> *7.10.2.1.2 The maximum speed shall be configurable and controlled by TCMS. This speed must also be supervised by ETCS (train related speed restriction associated to TCMS remote control mode).*

The authors share the safety concerns. In UC5.4-041, isolating ETCS-OB is provided only in agreement with IOM, as an exceptional procedure provided, by definition, to address exceptional conditions. Moving the train shall for instance permit to resume normal operations, which is always more desirable than a train immobilized in the middle of the track without functional ATP.

The use-case shall be considered under safety light. It may require consolidation with specific measures. It may be deleted: isolation by on-board personnel as today remains possible, so sending an on-board driver is always possible even if time-consuming.

R2: Safe Push

According to feedback 47 in [REV 01], a single push initiates a hand-over appeared too simple, as it could lead to unintentional accidents. A two-push sequence was suggested. Another solution could be to use separate buttons, with a long push for request and handover. These proposals intended to be more robust to human errors.

As no proposal appeared to the authors better than the other, the ‘Push’ was renamed ‘Safe Push’ in the introductory text and left open. Such an ergonomic optimization shall be defined according to WP6 task 6.7 consideration of human factors.

R3: Changing the train’s direction of travel only at standstill

In this document, a hand-over from driver to driver or to some automation is possible. Changing direction of travel of the train is not possible if the train is already moving. This technical assumption was implicit all along the document creation. Task 6.7/6.8 may investigate how this is realized.

R4: Forceful takeover by some on-board driver, e.g. at standstill

An ergonomic variant is that an on-board driver is allowed to take responsibility of the train without agreement by the remote driver currently in charge. This use case is particularly meaningful if this on-board driver has been sent to the train because remote control could not help anymore. It could also be the default train behaviour when a driver opens a cabin on a train at standstill. Such an ergonomic optimization shall be defined according to WP6 task 6.7 consideration of human factors.

R5: Braking or sounding the horn while monitoring a train

In current concept a monitoring driver, although not responsible for a train has the capability to brake or even brake in emergency. It forces a take-over from the previously controlling driver. A similar strategy is taken for sounding the horn.

This capability is given in case a monitoring driver sees a danger and requires stopping the train. The authors of this document could not imagine a scenario where somebody is on the track and

a monitoring driver tries to stop the train but lacks acknowledgement.

the monitoring driver issues a handover request

the controlling driver does not see the obstacle at first

is further distracted from the obstacle by the handover request issued above.

the person is hit although an early avoidance manoeuvre would have been possible, and may have saved the person.

Some partners found this behaviour a breach in the responsibility of the driver in control. This argument is particularly powerful if the monitoring drivers lack the competency expected by the driver in charge (self-control, understanding of responsibility).

A sound and documented Human Factor Analysis shall be performed on this topic in the context of WP6 task 6.7.

R6: Registering neighbouring RSC

The registration partner to neighbouring RCSs presented in this document intends to provide a seamless registration to the driver in charge, of for autonomous trains. It also permits that a train is visible at all centres in the train area. It is presented somewhat as a default. While the operational rules around responsivity distribution over multiple RSC get clearer, this protocol may be improved.

R7: Checking driver competency profiles

With the introduction of remote control, the authors feared that some driver takes control of a train he/she is not qualified for: while choosing,

- the workplace is the same for all trains,
- the train is now reduced to a name in a multiple-choice list rather than in front of the driver.

Therefore, a competency check was introduced before handover. It is performed by the train.

This partly bases on the choice of operational actors, partly on the intuition that the train is the ultimate instance deciding to start or not. Such checks can be implemented sooner (at RSC), or several times in the process. The driver's workplace may not even propose him/her vehicles he/she is not allowed to drive.

The current document does not exclude that the functional distribution performed during logical analysis redistributes the driver's competency check.

R8: Monitoring multiple trains

In this document, the main mission of remote drivers it to attend autonomous trains when the automation reaches degraded situations. This raises the question: what do the drivers when everything works perfectly? An answer is that remote drivers may monitor one or several trains between controlling assignments.

A 'static' allocation of drivers e.g., 1 driver for 6-8 trains, is a simple form of organisation. It is valid if a high number of remote drivers is available per train: monitoring efficiently many trains becomes cognitively difficult at some point, even with giant screens interleaving all video streams.

The driver will not be capable to take responsibility for those trains as if driving them. But attending the trains will certainly allow him/her a shorter time to adapt while taking control of the train – the driver knows where the train is, has an eye on the train's key figures. If answering calls by passengers, this information is already there.

A dynamic allocation of drivers can also be envisioned: with 40 trains per driver for example, displaying permanently each train for at least one driver does not make sense anymore: it would overload each single driver's cognition. Some work organisation, not defined prior to this document, may lead to a dynamic allocation of monitoring: monitoring a single train known for a technical

problem, or trains approaching some key location. Also, in that case, monitoring several trains may be desirable.

Lastly, drivers on call may not monitor trains between assignments, especially not multiple trains.

Monitoring multiple trains cannot be for safety reasons: when a driver concentrates on a train needing attendance, he/she leaves the monitored trains unmonitored – controlling a train requires full attention. If multiple monitoring was safety relevant, the left-alone trains would impair service, at least due to a time-consuming re-allocation to other drivers. So multiple monitoring has to aim at availability, quality of service, or all things important but interruptible.

Compared to single monitoring, multiple monitoring also introduces a breach in ergonomic paradigms: existing, proven in use ergonomic principles (desks, sound or visual notifications) aim at a driver focusing on a single train. Introducing multiple monitoring means among others solving the problem of attribution of several sources of alarms (see lost alarm policy section 3.8 p.46), reassessing the cognitive charge in stress situations. All things not solved in this document.

From the point of view of safety, if monitoring drivers remain allowed to brake the train or sound the horn, those actions shall be attributed to the train they monitor, unless distributed to all trains they monitor. The latter may lower dramatically operations performance.

This document addresses multiple monitoring at dedicated places where the topic seamed to emerge. Given the innovative mission of R2DATO WP5, no attempt was made to repress the topic. This document, however, does not intend to decide about multiple train monitoring.

Collected assumptions (presence of a RUS) or solutions (abstraction of a lost alarm policy to interface as openly as possible with some RU's workflow system) are documented.

It may raise the reader's awareness to this seemingly emerging topic.

The document tries to avoid decision, I.e., build no barriers that would forbid it.

The reader, however, should keep in mind that this topic is conditioned by aspects beyond the scope of current document (work organisation, human factor analysis), and probably even WP6 task 6.7.

R9: If a train is autonomy-capable, it may take control on its own initiative

Following all 3 states correspond to the functionality of an autonomous train, with a different responsibility:

OAS: ATO + PER/APM + ETCS fully functional	Remote driver	Driver responsibility
Yes	Uninvolved, Observing	None (GoA4)
Yes	Monitoring	Vigilance, if DMI permits it (Monitored GoA4)
Yes	Controlling	Full (Obstacle-assisted GoA2)

Is the ambiguity between Monitored GoA4 and Obstacle-Assisted GoA2 avoidable for the user?

For instance, if a driver driving manually with obstacle avoidance (PER+APM) under ETCS protection engages ATO, the train reaches Obstacle-assisted GoA2. Should it demote automatically the driver to Monitoring, I.e. enter 'Monitored GoA4'.

Current version sees this aspect as a DMI optimization: on the long term, it simplifies the number of driver transitions (ATO-Engage commands also RSC-Claimgrant LongPush). It also lowers the self-explaining character of the DMI by merging 2 independent state machines in one. For a first prototypal run, current solution without optimization is seen as equally good. On the long term, current optimization should be presented to drivers for evaluation *driven by real work*.

R10: If a train is standstill-standalone, a monitoring request automatically leads to control.

Same argument as above. This optimization, raised during review, is seen as potentially valuable for drivers in operations. For a first prototype run a self-explaining DMI remains valuable enough not to introduce a change of this magnitude in the document. On the long term, current optimization should be presented to drivers for evaluation *driven by real work*.

REFERENCES

[CYB] CLC/TS 50701:2023, Railway applications - Cybersecurity

[D5.2 UCs PER] D5.2 - Definition of use cases, operational parameters and scenarios for safe perception systems FP2-T5_2-D-FTS-040-01

[EN50126]

[GA] Grant Agreement, Project 101102001 - FP2 - R2DATO, 19/12/2022

[REV Ed01] Review Report about D5.4 Use-cases for remote control, FP2-T5_4-C-MER-011-01 (current document)

[SRDC TAURO] Specification of the Remote Driving and Command, Contract: H2020 – 101014984, Delivery: D2.1, TAU-T3_1-D-FTI-039-02, Revision: 05, Revision date: 14.06.2022

[SRS X2Rail-4 v0.2.4] X2Rail-4, WP5 GoA3/4 Specification version 0.2.4. Call S2R-CFM-IP2-01-2019, Deliverable D5.1, X2R4-WP05-D-ALS-010-009.

[SRS X2Rail-4 v0.3.0] X2Rail-4, WP5 GoA3/4 Specification version 0.3.0. Call S2R-CFM-IP2-01-2019, Deliverable D5.1, X2R4-WP05-D-ALS-010-009. Part of X2Rail-4 baseline 0.1.

[SRS TAURO 08] TAURO, Contract No. H2020 – 101014984, Specification of the Remote Driving and Command version 08, Deliverable D2.1, TAU-T2_1-D-CAF-004-07 (05/07/2022)

[SS-125] ERA * ERTMS/ATO - System Requirements Specification * SUBSET-125 v0.1.0

[STEST TAURO] Specification of the Remote Driving and Command, Contract: H2020 – 101014984, Delivery: D3.1, TAU-T2_1-D-CAF-004-07, Revision: 08, Revision date: 04.07.2022