# ETSI TR 122 990 V19.0.0 (2025-10)

TECHNICAL REPORT

**5G;**
**Study on off-network for rail**
**(3GPP TR 22.990 version 19.0.0 Release 19)**

Reference
RTR/TSGS-0122990vj00

Keywords
5G

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

***Important notice***

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

***Notice of disclaimer & limitation of liability***

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

# Legal Notice

This Technical Report (TR) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at 3GPP to ETSI numbering cross-referencing.

# Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

This document studies if further enhancements to the 5G system are feasible or not for the support of Off-Network for Rail.

This document collects all Off-Network use cases from SA1 Study on Future Railway Mobile Communication System (FRMCS) in order to refine them and new use cases to support Off-Network for Rail in clause 5 for Communication Applications.

The potential new service requirements are also consolidated in clause 5.

The results of gap analysis identify limitations, missing requirements and existing functionalities supported by 3GPP in clause 5.

Following the gap analysis, the assessment of technical feasibility, complexity and overhead of normative 3GPP adjustments to support limitations, missing requirements and functionalities as required by Off-Network for Rail is considered in clause 8.

Potential requirements are then consolidated in clause 9.

The conclusions and recommendations are proposed in clause 10 to conclude if further enhancements to the 5G system are needed and feasible for the support of Off-Network for Rail.

# 1 Scope

The present document analyses Rail Off-Network use cases in order to derive potential requirements and investigate if normative adjustments are feasible or not.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.289: "Mobile Communication System for Railways".

[3] 3GPP TS 22.179: "Mission Critical Push To Talk (MCPTT)".

[4] 3GPP TS 22.280: "Mission Critical Services Common Requirements (MCCoRe)".

[5] 3GPP TS 22.281: "Mission Critical Video services".

[6] 3GPP TS 22.282: "Mission Critical Data services".

[7] 3GPP TS 22.261: "Service requirements for the 5G system".

[8] 3GPP TS 22.185: "Service requirements for V2X services".

[9] 3GPP TS 22.186: "Enhancement of 3GPP support for V2X scenarios".

[10] UIC MG-7900: “Future Railway Mobile Communication System Use Cases”.

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ACRONYM> <Explanation>

# 4 Overview

The present document is a 900 series Technical Report (TR) written by 3GPP TSG SA WG1 (SA1). Such a TR is not normative, i.e. cannot be used for implementation directly. It is primarily written by SA1 to summarise the high-level Off-Network communication needs of the railway community and to identify the corresponding requirements.

**Rail Context**

Future rail communication is an important part of the digitalization of rail operations. In addition to network-oriented communication, this also includes that without involving the network. GSM-R already used this and was called Direct Mode to describe the ability of a User Equipment to communicate directly with each other, independent of the network.

Off-Network is a new terminology for the Rail sector, already introduced within 3GPP MCX specifications. UIC will promote the use of Off-Network to replace Direct Mode. But unfortunately, the terminology has slight differences in the meaning. For example, the Rail sector considers use of Off-Network communications where no network services are available either due to network failure (e.g. coverage, capacity, etc.) or due to lack of coverage (remote area's). In 3GPP MCX specifications, Off-Network communications can be setup even when network services are available.

In addition to voice communication, Off-Network communication will also increasingly be used for the exchange of train safety data in the future.

Examples of use cases which require Direct Mode:

- Automatic Train Protection (ATP) data communication
- Automatic Train Operation (ATO) data communication
- Critical real-time video
- Virtual Coupling data communication

Virtual Coupling data communication is the only use case where Off-Network is the intended mode of operation (also called “default mode”) even if the network is available.

All other use cases shall consider Network-Oriented mode as the default mode when the network is available (for the first and following attachments) and shifting to Off-Network when the network is not available.

# 5 Communication Applications related use cases

## 5.1 Introduction

This clause describes use cases of Communication Applications (e.g. Virtual Coupling data communication).

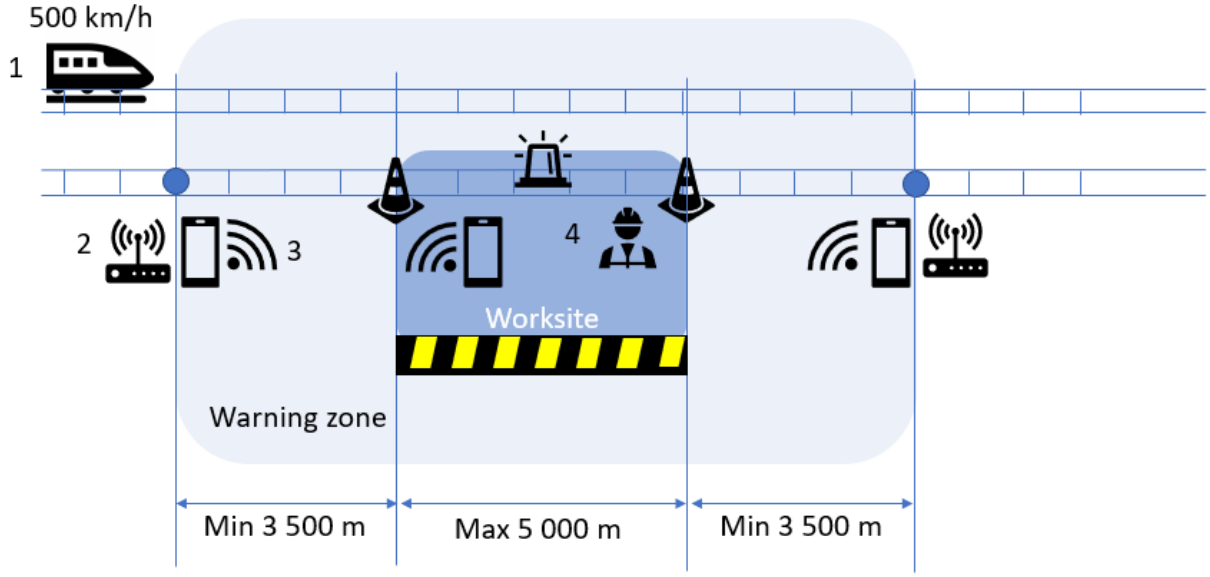
## 5.2 Trackside Maintenance Warning System communication

### 5.2.1 Description

Generally, trackside maintenance occurs during daily train operation. For safety reasons, trackside maintenance staff need to be informed about approaching trains entering the worksite. Thus, the intention of a trackside warning system is to inform trackside staff about the approaching train to keep rail capacity available while working on the tracks.

The trackside maintenance warning system consists of a single or multiple train detector entity(ies) (sensors, lookout man or interlocking station information + communication device), and a single or multiple warning entity(ies). The train detector entity is responsible to detect the approaching train and to trigger the alarm to the warning entities (as an option, the alarm should be triggered to a central/control entity also that relays the alarm to all warning entities). The warning entity indicates trackside workers about the approaching train on existing or adjacent tracks in form of visual signal e.g. flashing light and audio signal e.g. tone/horn. In large worksites or areas of high-speed trains, multiple warning entities can be spread out along the worksite to repeat the train approaching indication. In addition, the trackside maintenance staff will receive the train approaching indication on its FRMCS Equipment (i.e. wearable device).

When the train has cleared the warning zone, the indication is withdrawn automatically by the warning system, by the interlocking or manually by an authorised operator located inside or at the edge of the warning zone.




1. Train approaches warning zone
2. Train is detected by stationary trackside warning device (automatically) or look-out man (manually)
3. Stationary unit or look-out man sends warning to [1..30] worker(s) (via stationary trackside warning device(s) or via personal UE(s))
4. Warning receives at worksite not less than 25 seconds (time for worker(s) to protect themselves)

**Figure 5.2.1-1: Description of the Trackside Maintenance Warning System**

Train detector entities and warning entities constitute the warning system that requires secured/safe continuous radio transmission of data between the sensors and the warning entities (e.g. keep alive messages for robustness and location information of entities/workers to differentiate between the tracks with a lateral distance accuracy of less than 1 meter). In addition, it encompasses the secured/safe radio transmission of the train approaching indication (i.e. start/stop transmitting the indication to the track workers) among the warning system and the FRMCS Equipment of the trackside staff. Train detection is outside scope of the warning system.

Due to the fact that such a warning system deployment is temporary and on-network communication services are not always available at the track, the FRMCS System provides necessary off-network communication services for the trackside warning system. Trackside maintenance warning system in off-network mode is well suited for small, short-term construction sites but should also be relevant for large and long-term construction sites.

The maximum train speed in the warning zone is 500 kmph.

Note: no speed limit applies in worksites in some Countries.

Communications between train detector entities located at both edges of the warning zone are not supported by the Trackside maintenance warning system.

As a deployment option, communication between the approaching train and the trackside warning system should be supported to e.g. avoid train detectors.

Fixed and moving worksites e.g. carrying out inspection work are supported by the Trackside maintenance warning system.

One-way (i.e. one train detector entity) and two-way (i.e. two train detector entities) traffic protection are supported by the Trackside maintenance warning system.

The minimum configuration of a warning system is:

- One train detector entity located closed or inside the worksite (i.e. detection by visual detection)
- One warning entity located inside the worksite

The maximum configuration of a warning system is:

- Two train detector entities located at both edges of the warning zone
- The maximum number of warning entities is 30, located inside the worksite
- The maximum number of workers (e.g. wearing warning devices through FRMCS Equipment) located inside the worksite is 50.

Different groups of workers can work at the same time along the worksite.

Workers or work group can join/leave the worksite based on their locations.

The warning system shall be flexible enough to easily setup.

Energy efficiency of the warning system for battery-powered entities is not supported.

Configuration and control of the warning system shall be available locally.

Configuration and control of the warning system should be available through on-network communication.

Positioning of the train detectors with accurate distance from the worksite is in the scope of the warning system with distance accuracy of +/- 1 meter.

The trackside maintenance warning system communication shall be reliable in tunnels, in bad weather conditions and in unfavourable geographical conditions.

Multiple and flexible use of spectrum bands shall be supported.

### 5.2.2 Pre-conditions

The FRMCS Users as part of the warning system are authorised to initiate, transmit/receive data and terminate the trackside maintenance warning system communication.

### 5.2.3 Service Flows

The entitled FRMCS User initiate, transmit/receive and terminate the trackside maintenance warning system communication.

A secure data communication application is used for the trackside maintenance warming system communication. The communication requests the QoS class which matches the application category of XXX within the FRMCS System.

Editor's note: applications categories applicable to Off-Network communications will be an outcome of the present study.

The arbitration is managed by the Arbitration application.

Editor's note: the Arbitration application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The metadata are recorded by the Data recording application.

Editor's note: the Data recording application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The communication is secured by the Assured data communication.

Editor's note: the Assured data communication use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The identities, presence and functional addressing is managed by the Role management & presence.

Editor's note: the Role management & presence use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The authorisation of communication is managed by the Authorisation of communication.

Editor's note: the Authorisation of communication use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The authorisation of application is managed by the Authorisation of application.

Editor's note: the Authorisation of application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The location of the FRMCS Equipment is managed by the Location services.

Editor's note: the Location services use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

### 5.2.4 Post-conditions

The entitled FRMCS User(s) as part of the warning system is able to securely exchange data in the appropriate area to intended FRMCS User(s).

### 5.2.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [32], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

### 5.2.6 Potential New Requirements needed to support the use case and gap analysis

#### 5.2.6.1 Requirements related to the Service layer

Editor's note : the following potential new MCX requirements are relevant for SA6.

[PR 5.2.6.1-1] The FRMCS System shall be able to initiate data communication for Trackside Maintenance Warning System to FRMCS Users upon a request from a functional identity entitled to initiate such communication.

[PR 5.2.6.1-2] The FRMCS System shall be able to select FRMCS user(s) to deliver the Trackside Maintenance Warning System data based on their functional identity and location either periodically or as a onetime request.

[PR 5.2.6.1-3] The FRMCS System shall allow FRMCS Users to join an ongoing data communication for Trackside Maintenance Warning System based on their functional identity and location.

[PR 5.2.6.1-4] The FRMCS System shall allow FRMCS Users to leave an ongoing data communication for Trackside Maintenance Warning System based on their functional identity and location.

[PR 5.2.6.1-5] The FRMCS System shall be able to terminate data communication for Trackside Maintenance Warning System upon a request received from a functional identity entitled to terminate the communication.

[PR 5.2.6.1-6] The FRMCS System shall allow configuration (e.g. functional identities of maintenance staff and warning entities) and control of the Trackside Maintenance Warning System when the FRMCS Equipment are served by a 3GPP RAT.

[PR 5.2.6.1-7] The FRMCS System shall allow configuration (e.g. functional identities of maintenance staff and warning entities) and control of the Trackside Maintenance Warning System when the FRMCS Equipment are not served by a 3GPP RAT.

### 5.2.6.2 Requirements related to the Transport layer

Editor's note : the following potential new requirements are relevant for SA2 and RAN.

[PR 5.2.6.2-1] The FRMCS System shall support the following traffic characteristics of data transfer for data communication for Trackside Maintenance Warning System:

Note: This table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (note 6) | Service area dimension (note 3) |
|---|---|---|---|---|---|---|---|---|---|
| Trackside maintenance warning system Communication | ≤500 ms | 99,9999% (note 7) | Stationary (warning system entities) and pedestrians (workers). Option: ≤500kmph for train detection via onboard system | 10 kbps up to 500 kbps | Small to medium | Up to 10 Mbps /km | ≤80/worksite | ≥8.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (note 4) | ≥12 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (note 5) |

NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.
NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.
NOTE 3: Estimates of maximum dimensions.
NOTE 4: Distance is equal to the distance for train of maximum speed of 500 kmph to enter the worksite + the maximum distance of a worksite
NOTE 5: Minimum distance of the warning zone
NOTE 6: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.
NOTE 7: Reliability figures could be achieved using multiple 3GPP 5GS-compatible spectrum bands simultaneously.

**Table 5.2.6.2-1: Traffic characteristics for Trackside Maintenance Warning System**

## 5.3 Remote Control of Engines communications

### 5.3.1 Description

It shall be possible for a remote driver to operate/control an engine (e.g. control movement and speed) of a vehicle typically for shunting operation in depots, shunting yards and/or for banking via a ground-based system or an on-board system located at opposite ends of the engine.

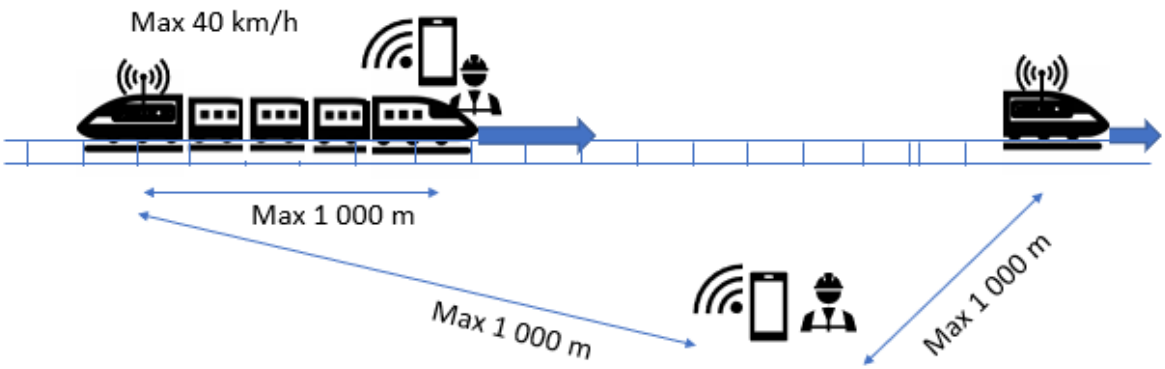



**Figure 5.3.1-1: Description of the Remote Control of Engines**

**Figure 5.3.1-2: Pictures of the Remote Control of Engines in operation**

Onboard system should have a distinct and unambiguous audible or visual warning device that indicates to nearby personnel that the vehicle is under active remote control and subject to movement.

Remote driver/ground-based entity and controlled engine(s)/onboard entity constitute the remote control of engines system that requires secured/safe continuous radio transmission of data between the remote driver and the controlled engine(s)s (e.g. keep alive messages for robustness, dynamic speed and brake control, report direction of travel and speed of the vehicle).

A remote driver shall be able to control up to 10 engines but only one engine at a time. To supply sufficient power, a locomotive may consist of one or more engines operated from a single remote driver. In that case, commands from the remote control shall be synchronized. A single onboard system is used to control the engines. Only one communication from the remote driver to the onboard system is required.

A remote driver having the capability to control more than one engine should have a mean to prevent simultaneous control over more than one locomotive.

If on-network mode is available, the remote driver shall be able to exchange data with the traffic control system to automatically operate the track switches to free the tracks before remotely operating the train.

If on-network mode is available, trains have to be geographically tracked by the traffic control system to prevent from traveling past predetermined boundaries (i.e. remote control zones to e.g. avoid other train movements).

If on-network mode is available, the system shall alert the traffic control system when a safety case happens to the remote driver (e.g. remote driver down) including the accurate location of the remote driver.

As an option, real-time video monitoring of tracks from onboard system in the cab or from trackside to the remote driver should be required simultaneously to the transmission of data for remote control of engines.

The remote control of engines is designed to be fail-safe so that if communication is lost the vehicle is brought to a stop automatically.

Due to the fact that very low latency is required, and on-network communication services are not always available at the depot, the FRMCS System provides necessary off-network communication services for the remote control of engines even if on-network communication services are available.

The maximum speed of the train remotely controlled shall be restricted not to exceed 40 kmph.

The remote control of engines shall be flexible enough to easily setup.

Configuration and control of the remote control of engines shall be available locally.

It shall be possible for a remote driver to awaken an onboard entity.

The remote control of engines communication shall be reliable in depots, in tunnels, with clear line of sight.

Multiple and flexible use of spectrum bands shall be supported.

As an option, the remote control application should be used to remotely control by maintenance staff other equipment such as overhead cranes in depots, see below:

**Figure 5.3.1-3: Alternative of Remote Control Application**

The remote control of overhead cranes has the same requirements on communication characteristics as the remote control of engines.

## 5.3.2 Pre-conditions

The FRMCS User is authorised to initiate, transmit/receive data/video and terminate the remote control of engines communication.

## 5.3.3 Service Flows

The entitled FRMCS User initiate, transmit/receive and terminate the remote control of engines communication.

A secure data communication application is used for the remote control of engines communication. The communication requests the QoS class which matches the application category of XXX within the FRMCS System.

Editor's note: applications categories applicable to Off-Network communications will be an outcome of the present study.

The arbitration is managed by the Arbitration application.

Editor's note: the Arbitration application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The metadata are recorded by the Data recording application.

Editor's note: the Data recording application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The communication is secured by the Assured data communication.

Editor's note: the Assured data communication use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The identities, presence and functional addressing is managed by the Role management & presence.

Editor's note: the Role management & presence use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The authorisation of communication is managed by the Authorisation of communication.

Editor's note: the Authorisation of communication use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The authorisation of application is managed by the Authorisation of application.

Editor's note: the Authorisation of application use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

The location of the FRMCS Equipment is managed by the Location services.

Editor's note: the Location services use case in Off-Network mode is FFS in the context of FS_OFFNETRAIL.

### 5.3.4 Post-conditions

The entitled FRMCS User is able to securely exchange data/video in the appropriate area to intended FRMCS User(s).

### 5.3.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [3], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

### 5.3.6 Potential New Requirements needed to support the use case

#### 5.3.6.1 Requirements related to the Service layer

Editor's note : the following potential new MCX requirements are relevant for SA6.

[PR 5.3.6.1-1] The FRMCS System shall be able to initiate data communication for Remote Control of Engines to FRMCS User(s) upon a request from a functional identity entitled to initiate such communication.

[PR 5.3.6.1-2] The FRMCS System shall be able to select one or multiple FRMCS user(s) to deliver the Remote Control of Engines data based on their functional identity and location either periodically or as a onetime request.

[PR 5.3.6.1-3] The FRMCS System shall be able to limit the number of FRMCS User(s) to be selected to deliver the Remote Control of Engines data at any one time.

[PR 5.3.6.1-4] An entitled FRMCS User shall be able to awake an FRMCS Equipment.

[PR 5.3.6.1-5] The FRMCS System shall be able to terminate data communication for Remote Control of Engines upon a request received from a functional identity entitled to terminate the communication.

[PR 5.3.6.1-6] The FRMCS System shall allow local configuration (e.g. functional identities of engines and remote drivers) and control of the Remote Control of Engines even when the FRMCS Equipment is served by a 3GPP RAT.

### 5.3.6.2 Requirements related to the Transport layer

Editor's note : the following potential new requirements are relevant for SA2 and RAN.

[PR 5.3.6.2-1] If the FRMCS Equipment is served by a 3GPP RAT, using NR for direct communication for Remote Control of Engines shall not interfere with on-network services.

[PR 5.3.6.2-2] The FRMCS System shall support the following traffic characteristics for communication for Remote Control of Engines:

Note: This table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (note 4) | Service area dimension (note 3) |
|---|---|---|---|---|---|---|---|---|---|
| Remote control of engines data communication | ≤10 ms | 99,9999% (note 4) | Stationary (trackside remote driver) and ≤40kmph (onboard remote control system and onboard remote driver) | 100 kbps up to 1 Mbps | Small to Medium | Up to 100 Mbps/km | 2 (remote driver and onboard system) | ≤1000m along rail tracks including depots and tunnels with clear line of sight | ≤2000m along rail tracks including depots and tunnels with clear line of sight |
| Remote control of engines video communication | ≤100 ms | 99,9% (note 4) | Stationary (trackside remote driver) and ≤40kmph (onboard remote control system and onboard remote driver) | 10 Mbps | Medium | Up to 1 Gbps/km | 2 (remote driver and onboard system) | ≤1000m along rail tracks including depots and tunnels with clear line of sight | ≤2000m along rail tracks including depots and tunnels with clear line of sight |

NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.
NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.
NOTE 3: Estimates of maximum dimensions.
NOTE 4: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.
NOTE 5: Reliability figures could be achieved using multiple 3GPP 5GS-compatible spectrum bands simultaneously

**Table 5.3.6.2-1: Traffic characteristics for Remote Control of Engines**

## 5.4 Train integrity monitoring data communication

### 5.4.1 Description

The Train Integrity is an on-board function responsible for verifying the completeness of a train composition, while the train is in operation, to guarantee safety on tracks. Train integrity consists concretely in monitoring the status of the train's tail to check that last wagon is regularly advancing in a coherent way in relation to the movement of the remaining train. The event of accidental train separation constitutes a serious danger for the next train, being a possible unexpected obstacle on the line, and therefore it needs to be promptly reported to the rail signalling system.

The main difference between train integrity monitoring in on-network mode and off-network mode consists in train integrity criteria that (1) is based on communication liveliness in on-network mode, whereas (2) requires verifying train tail coherent movement respect to front cabin, based on train tail odometry data (i.e. position, speed or acceleration of train tail and front cabin) in off-network mode. In fact, off-network communication between train tail and front cabin could be present also after train splitting with limited distance of separated waggons.

## 5.4.2 Pre-conditions

The On-board Train Integrity (OTI) entities (i.e. the FRMCS Users) are authorised to initiate Train Integrity Monitoring Data Communication.

## 5.4.3 Service Flows

James is the lead driver of a cargo train of 1 000 metres long with 50 wagons that are not fully equipped with power supply.

The front cabin, the train tail wagon and, optionally some or all of the intermediate wagons to offer more flexibility in train composition, are equipped with On-board Train Integrity (OTI) entities connected to UEs in off-network mode at the lower part of the wagons (i.e. no direct line-of-sight between OTI entities). UEs may not be dedicated to On-board Train Integrity.

James powers on the front cabin before starting to operate the train. The OTI entities establish communications with each other and begin exchanging status (i.e. position, speed or acceleration information, and if supported wagon diagnostic information) via the connected UEs in off-network mode. The train integrity status is “Confirmed” (all wagons connected and operational). The Train Integrity system shall avoid pairing James’ OTI entities with other trains’ OTI entities in proximity.

Train Integrity data exchanges are encrypted to prevent eavesdropping.

Train Integrity data exchanges are recorded in case something bad happens (e.g. wrong pairing between OTI entities) and somebody wants to review the incident later.

James starts running its train to its destination on non-electrical lines where there is no network coverage. The Train Integrity Monitoring procedure restarts every 30 seconds (configurable timer) until the train stops running.

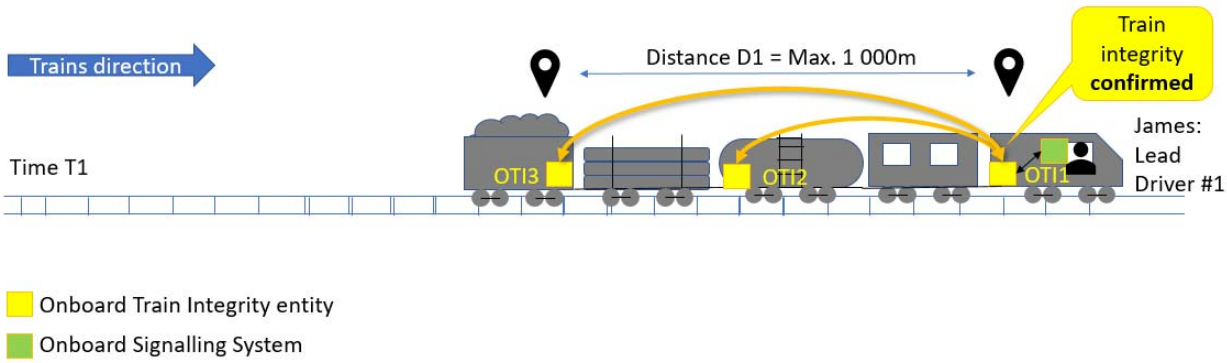



**Figure 5.4.3-1: Train integrity confirmed**

For some reason, the train tail splits off of James’ train. The Train Integrity system detects the event and the train integrity status becomes “Lost”.

In the meantime, James is communicating with its train operating centre to prepare its next mission. The Train Integrity system informs on-board signalling system about train integrity status. The on-board signalling system takes priority on James ongoing communication to inform him thus allowing him to intervene rapidly and appropriately (e.g. reducing the speed and breaking the train in a safe location).

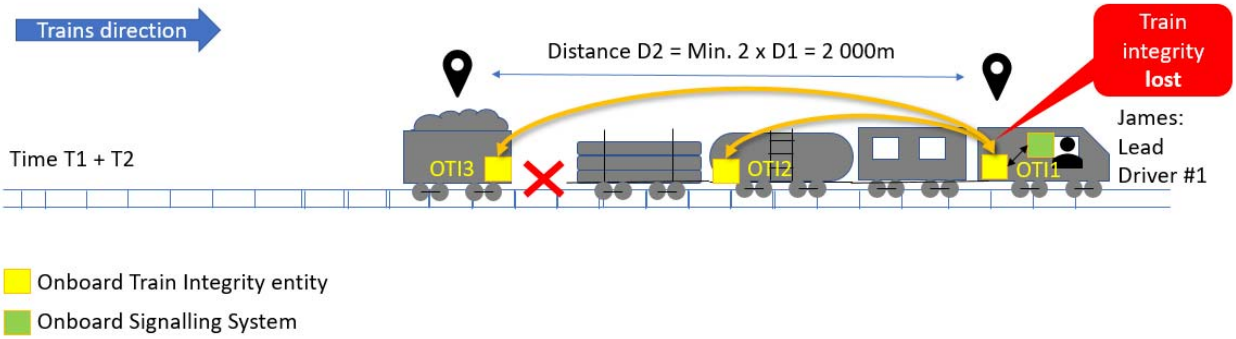



**Figure 5.4.3-2: Train integrity lost**

## 5.4.4 Post-conditions

Train integrity status can be continuously exchanged between On-board Train Integrity (OTI) entities to warm accidental train separation and avoid any rail safety issue.

## 5.4.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [3], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

## 5.4.6 Potential New Requirements needed to support the use case

### 5.4.6.1 Requirements related to the Service layer

[PR 5.4.6.1-1] The FRMCS Service in Off-Network mode shall be able to initiate data communication for Train Integrity Monitoring to relevant FRMCS Users upon a request from a functional identity entitled to initiate such communication.

[PR 5.4.6.1-2] The FRMCS Service in Off-Network mode shall provide the necessary communication means to support Train Integrity Monitoring.

[PR 5.4.6.1-3] The FRMCS Service in Off-Network mode shall allow arbitration for Train Integrity Monitoring communication.

[PR 5.4.6.1-4] The FRMCS Service in Off-Network mode shall allow FRMCS Users to join an ongoing data communication for Train Integrity Monitoring based on their functional identity and location.

[PR 5.4.6.1-5] The FRMCS Service in Off-Network mode shall allow FRMCS Users to leave an ongoing data communication for Train Integrity Monitoring based on their functional identity and location.

[PR 5.4.6.1-6] The FRMCS Service in Off-Network mode shall provide means to obtain and exchange odometry information of FRMCS Users (e.g. position, speed or acceleration).

[PR 5.4.6.1-7] When an FRMCS Equipment in Off-Network mode is simultaneously used by multiple FRMCS Users, each of the FRMCS Users shall be individually addressable.

[PR 5.4.6.1-8] The FRMCS Service in Off-Network mode shall be able to terminate data communication for Train Integrity Monitoring upon a request received from a functional identity entitled to terminate such communication.

[PR 5.4.6.1-9] The FRMCS Service in Off-Network mode shall provide the means to record Train Integrity Monitoring data communication and communication related information (e.g. FRMCS Users involved) to an external system.

[PR 5.4.6.1-10] The FRMCS Service Security Framework shall provide mechanisms in Off-Network mode to cover identity management, authentication, authorisation and data protection in respect to Train Integrity Monitoring.

### 5.4.6.2 Requirements related to the Transport layer

[PR 5.4.6.2-1] The FRMCS Equipment power consumption in Off-Network mode shall be minimised.

[PR 5.4.6.2-2] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of data transfer for direct data communication for Train Integrity Monitoring:

Note: This table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (Note 3) | Service area dimension (Note 4) |
|---|---|---|---|---|---|---|---|---|---|
| Train integrity monitoring data Communication | ≤1 s | 99,9% | ≤350k mph | 10 kbps up to 500 kbps | Small to Medium | Up to 25 Mbps /km | ≤50/train | ≤2 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) (Note 6) | ≤2 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) (Note 6) |

NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.
NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.
NOTE 3: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.
NOTE 4: Estimates of maximum dimensions.
NOTE 5: Distance is equal to twice the maximum length of a train to cover train tail split
NOTE 6: Non-Line-of-Sight (NLOS) between UEs shall be supported.

**Table 5.4.6.2-1: Traffic characteristics for Train Integrity Monitoring**

## 5.5 Shunting communication

### 5.5.1 Description

Changing the locomotive of a train, coupling/uncoupling wagons, changing the order in which wagons are arranged in a train are all kinds of shunting movements. Shunting movements can be differentiated from other regular movements: this main point of differentiation is that almost all shunting is done within a single station or a shunting yard.

Shunting movements between shunting members can be ordered by radio, in on-network or in off-network modes. This section describes shunting communications in off-network mode where a ground user e.g. controller/dispatcher is not necessary.

### 5.5.2 Pre-conditions

The Shunting members (i.e. the FRMCS Users) of the shunting team #1 (i.e. Shunting Service Area #1 and Shunting Team ID #1) are authorised to initiate Shunting Communications.

### 5.5.3 Service Flows

A cargo train has to prepared by coupling the main locomotive to the rest of the wagons. A Shunting Service Area is defined to avoid any other train movements in the same area. There is no network coverage in this Shunting service area.

Bob has been assigned the role of the shunting leader of a shunting team in charge of this operation. Bob prepares its mission together with James, which has been assigned the role of the shunting driver. The shunting team members are all equipped with a Shunting device connected to a UE. They are operating their UEs in off-network mode and have selected their role and shunting service area to enable voice and data exchanges between the shunting members. The Shunting group voice and data communications are encrypted to prevent eavesdropping.

Bob exchanges with the shunting members secured and reliable information required to perform safe shunting movements of trains, (e.g. issuing route requests, route confirmation, giving driving commands, confirmation for driving commands, etc.). Bob receives confirmation upon successful reception of the message for all shunting members.

Service Flow#1 (shunting movements ordered by human): James, located in the front cabin (indoor) and without direct line-of-sight of the track, pushes a group of wagons (i.e. going backwards), continuously and securely ordered by Bob, located at train tail (outdoor or indoor) as a lookout man. To do so, Bob enables an assured safety link function that periodically send tones or keep alive messages to the shunting members. Bob may shout orders periodically into his Shunting device. Bob's orders take priority on the periodic assured safety link tones and every team member is able to hear him.

If the voice/data can not be exchanged for more than 2 seconds (configurable time), every member of the shunting team is informed, thus allowing them to intervene rapidly and appropriately (e.g. James breaking the train).

When Bob orders James to stop its train, he disables the assured safety link function and invites Dave, a member of another shunting team located on the trackside, to be part of their shunting team to couple James' train to the rest of the wagons. Shunting team members of both teams are now part of the same shunting team.

Dave, James and Bob are simultaneously talking to each other to couple James' train safely.

Dave notices that another worker is in the area and, to avoid collision with James' train shouts a warning into his UE. Dave's warning takes priority, and member of the shunting team is able to hear him to intervene rapidly and appropriately (e.g. James breaking the train).

Shunting communications are recorded (e.g. shunting members composition) in case something bad happens and somebody wants to review the incident later.

Service Flow#2 (shunting movements self-controlled using video by the driver): James, located in the front cabin (indoor) and without direct line-of-sight of the track, pushes a group of wagons (i.e. going backwards), continuously and securely monitoring the track using video communication with camera connected to a UE located at the train tail.

If the video can not be exchanged for more than 2 seconds (configurable time), James is informed, thus allowing him to intervene rapidly and appropriately (e.g. James braking the train).

Shunting video communications are recorded (including metadata e.g. timestamp, originator, receiver, roles) in case something bad happens and somebody wants to review the incident later.

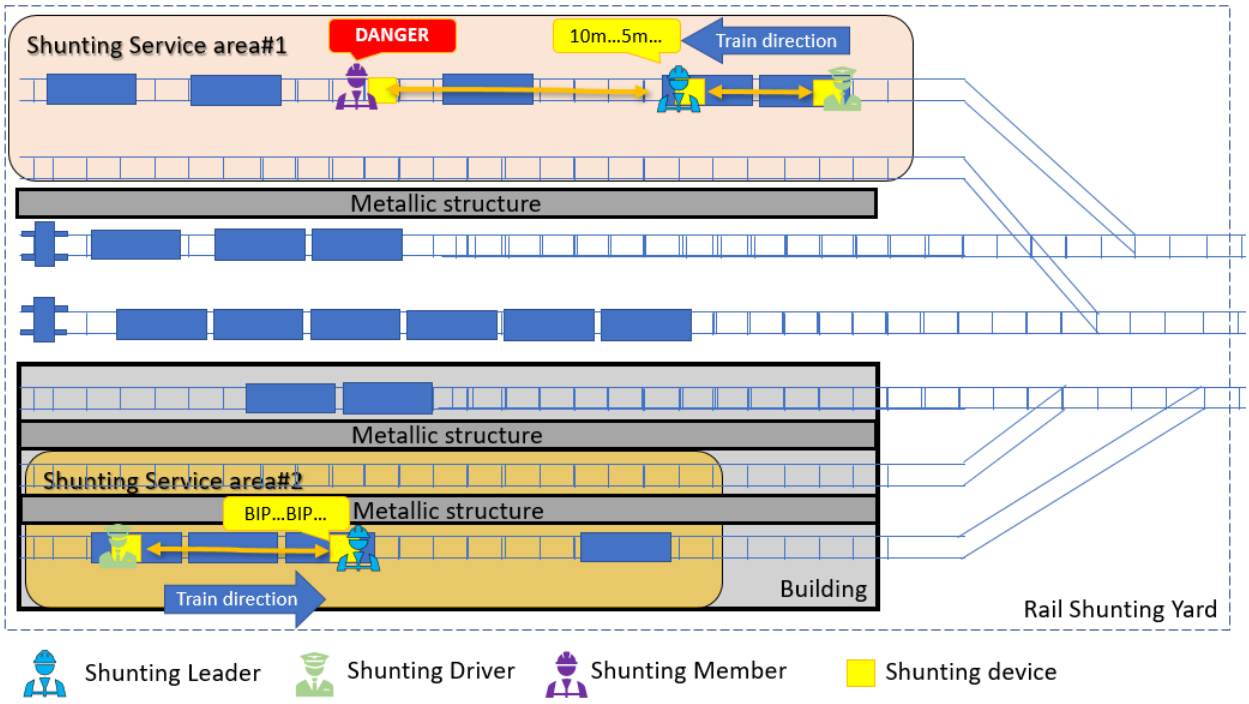



**Figure 5.5.3-1: Examples of Shunting communications**

## 5.5.4 Post-conditions

Shunting movement orders can be continuously exchanged between the Shunting members of the shunting team to avoid any rail safety issue while shunting.

Shunting videos can be continuously exchanged between the Driver and the shunting cameras to avoid any rail safety issue while shunting.

## 5.5.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [3], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

## 5.5.6 Potential New Requirements needed to support the use case

### 5.5.6.1 Requirements related to the Service layer

[PR 5.5.6.1-1] The FRMCS Service in Off-Network mode shall be able to initiate voice, data and video communication for Shunting movements to relevant FRMCS Users upon a request from a functional identity entitled to initiate such communication.

[PR 5.5.6.1-2] The FRMCS Service in Off-Network mode shall provide the necessary communication means to support Shunting.

[PR 5.5.6.1-3] The FRMCS Service in Off-Network mode shall allow the multi-talker control.

[PR 5.5.6.1-4] The FRMCS Service in Off-Network mode shall provide the means to enable/disable continuous monitoring of the communication links to all involved FRMCS Users of a specific voice, data or video group communication.

[PR 5.5.6.1-5] An authorised FRMCS User in Off-Network mode shall be able to enable/disable continuous monitoring of the communication links to all involved FRMCS Users of a specific voice, data or video group communication.

[PR 5.5.6.1-6] If a degradation or loss of a communication link is detected, the remaining FRMCS Users shall be informed. The ongoing communications among the remaining FRMCS Users shall continue.

[PR 5.5.6.1-7] The FRMCS Service in Off-Network mode shall allow arbitration for Shunting communication.

[PR 5.5.6.1-8] The FRMCS Service in Off-Network mode shall allow FRMCS Users to join an ongoing voice and data communication for Shunting based on their functional identity and location.

[PR 5.5.6.1-9] An authorised FRMCS User shall be able to invite another FRMCS User to join a voice communication, based on his functional identity, FRMCS User Identity, or FRMCS Equipment Identity, even if his already involved in another active communication.

[PR 5.5.6.1-10] When accepting a communication invitation, in case the FRMCS User has an active voice communication, the FRMCS User shall be able to leave, terminate or merge the voice communication(s).

[PR 5.5.6.1-11] The FRMCS User sending the invitation shall be informed if the targeted FRMCS User receives, accepts, rejects or ignores the invitation.

[PR 5.5.6.1-12] All involved FRMCS User shall be informed when group communication status of an FRMCS user changes e.g. join, leave, on hold, terminate, invite, merge.

[PR 5.5.6.1-13] The FRMCS Service in Off-Network mode shall allow FRMCS Users to leave an ongoing voice and data communication for Shunting based on their functional identity and location.

[PR 5.5.6.1-14] The FRMCS Service in Off-Network mode shall be able to terminate voice, data and video communication for Shunting upon a request received from a functional identity entitled to terminate such communication.

[PR 5.5.6.1-15] The FRMCS Service in Off-Network mode shall provide the means to record Shunting communication and communication related information (e.g. FRMCS Users involved and their roles) to an external system.

[PR 5.5.6.1-16] The FRMCS Service Security Framework shall provide mechanisms in Off-Network mode to cover identity management, authentication, authorisation and data protection in respect to Shunting.

### 5.5.6.2 Requirements related to the Transport layer

[PR 5.5.6.2-1] The FRMCS Service in Off-Network mode shall not interfere with FRMCS Services in On-Network mode.

[PR 5.5.6.2-2] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of voice, data and video transfer for direct communication for Shunting:

Note: this table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (Note 3) | Service area dimension (Note 4) |
|---|---|---|---|---|---|---|---|---|---|
| Shunting voice Communication | ≤100 ms | 99,9999% | ≤40 kmph | 100 kbps up to 300 kbps | Small | Up to 1 Mbps/line km | ≤10 shunting members | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) |
| Shunting data Communication | ≤500 ms | 99,9999% | ≤40 kmph | 10 kbps up to 500 kbps | Small to medium | Up to 10 Mbps/km | ≤10 shunting members | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) |
| Shunting video Communication | ≤100 ms | 99,9% | ≤40 kmph | 10 Mbps | Medium | Up to 100 Mbps/km | ≤10 | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) | ≤1.5 km along rail tracks including tunnels, bad weather conditions and unfavourable geographical conditions (Note 5) |

NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.
NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.
NOTE 3: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.
NOTE 4: Estimates of maximum dimensions.
NOTE 5: Non-Line-of-Sight (NLOS) between UEs, UE to UE both inside locomotives and unfavourable radio propagation conditions in shunting yards shall be supported.

**Table 5.5.6.2-1: Traffic characteristics for Shunting communications**

# 5.6 Train ready for departure communication

## 5.6.1 Description

Station departure and the platform/train interface is one of the biggest risk areas in railway operations today.

Rail operators implement various different processes for managing station departure with similar objective of ensuring that passengers are safely onboard the train and that the train can safely depart the platform.

Train departure communications includes (1) driver to controller communication and (2) conductor to driver communication. Train ready message sent from the driver to the controller is typically used in main railway stations, in on-network mode. Train ready for departure from a platform involving platform staff (e.g. chief conductor) and driver sent from the platform staff to the driver, is typically used in remote station e.g. rural area, in off-network mode. Another train ready for departure communication scenario in remote stations involves the driver and platform camera(s) to check closing doors and that no passengers are left on the platform without any platform staff.

This section describes Train ready for departure communications in off-network mode. No service handover between on-network and off-network modes is foreseen.

## 5.6.2 Pre-conditions

The Chief conductor (i.e. the FRMCS User) is authorised to initiate Train ready for departure Communications.

## 5.6.3 Service Flows

Monday, 9:30 in the morning. James has been assigned the role of the lead driver of train #12345. His train #12345 stands in platform A, located in a rural railway station where there is no network coverage. The train is ready for boarding. His train should leave at 10:00. James is located in the front cabin (indoor).

Service Flow#1 (driver and platform staff): Bob has been assigned the role of the chief conductor in charge of ensuring a safe boarding for passengers. He stands in platform A, near the train tail.

James and Bob are equipped with devices connected to a UE. They are operating their UEs in off-network mode and have selected their role and platform area to enable data exchanges between each other. The data communications are encrypted to prevent eavesdropping.

Passengers are boarding.

09:59. Train is ready for departure but Bob notes that a Family is running not to miss train #12345. 10:03. All passengers are onboard. Doors are closing. When all doors are safely closed, Bob sends a secured and reliable “Train #12345 is ready for departure” message to James. Bob receives confirmation upon successful reception of the message by James. James acknowledges the message and starts running his train.

Train ready for departure message is recorded (e.g. timestamp, originator, receiver, roles, content) in case something bad happens and somebody wants to review the incident later.

Service Flow#2 (driver and platform camera(s)): two fixed cameras are located on platform A. Camera C1 is located one near the train tail, camera C2 is located at the front cabin. Each camera is connected to a UE operating in off-network mode. Each camera has automatically selected its role and platform area (via static or dynamic configuration) to enable video exchanges with the driver’s UE. The video communication is encrypted to prevent eavesdropping.

Passengers are boarding.

09:59. Train is ready for departure, but a Family is running not to miss train #12345. 10:03. All passengers are onboard. James enables video from camera C1 to check passengers on the platform. Then James switch video from camera C1 to C2. James may also enable video from both cameras C1 and C2. Doors are closing. When all doors are safely closed, James disable videos from cameras C1 and C2. James starts running his train.

Train ready for departure video is recorded (including metadata e.g. timestamp, originator, receiver) in case something bad happens and somebody wants to review the incident later.

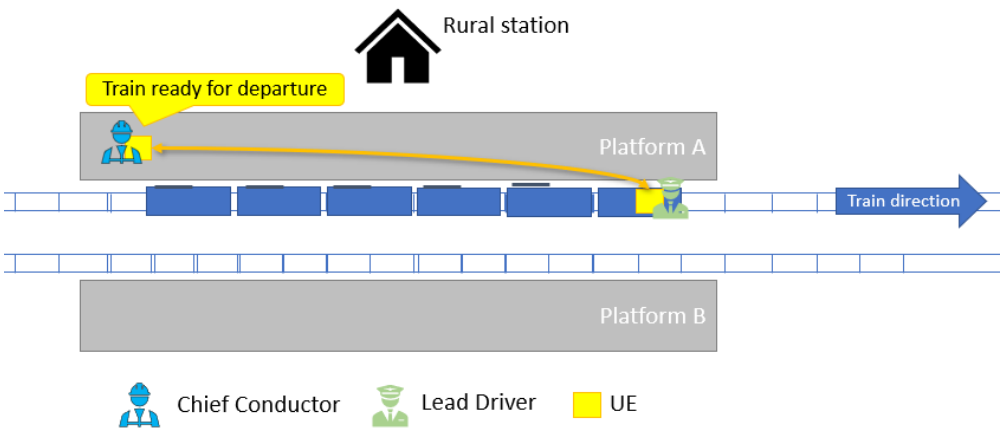



**Figure 5.6.3-1: Train ready for departure communications**

## 5.6.4 Post-conditions

Train ready for departure messages are safely exchanged between the Chief Conductor and the Lead Driver to avoid any safety related issue for passengers before departure.

Train ready for departure videos are safely exchanged between the Chief Conductor and the Fixed Cameras to avoid any safety related issue for passengers before departure.

## 5.6.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [3], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

## 5.6.6 Potential New Requirements needed to support the use case

### 5.6.6.1 Requirements related to the Service layer

[PR 5.6.6.1-1] The FRMCS Service in Off-Network mode shall be able to initiate data and video communications for Train Ready for Departure to relevant FRMCS User upon a request from a functional identity entitled to initiate such communication.

[PR 5.6.6.1-2] The FRMCS Service in Off-Network mode shall provide the necessary communication means to support Train Ready for Departure.

[PR 5.6.6.1-3] The FRMCS Service in Off-Network mode shall allow arbitration for Train Ready for Departure communication.

[PR 5.6.6.1-4] The FRMCS Service in Off-Network mode shall be able to terminate data and video communications for Train Ready for Departure upon a request received from a functional identity entitled to terminate such communication.

[PR 5.6.6.1-5] The FRMCS Service in Off-Network mode shall provide the means to record Train Ready for Departure communication and communication related information (e.g. FRMCS Users involved and their roles) to an external system.

[PR 5.6.6.1-6] The FRMCS Service Security Framework shall provide mechanisms in Off-Network mode to cover identity management, authentication, authorisation and data protection in respect to Train Ready for Departure.

### 5.6.6.2 Requirements related to the Transport layer

[PR 5.6.6.2-1] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of data and video transfer for direct communication for Train Ready for Departure:

Note: This table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (Note 3) | Service area dimension (Note 4) |
|---|---|---|---|---|---|---|---|---|---|
| Train Ready for Departure data Communication | ≤500 ms | 99,9% | Stationary | 10 kbps up to 500 kbps | Small to medium | Up to 10 Mbps /km | 2 | ≤1 000 m along rail tracks including bad weather conditions (Note 5) | ≤1 000 m along rail tracks including bad weather conditions (Note 5) |
| Train Ready for Departure video Communication | ≤100 ms | 99,9% | Stationary | 10 Mbps | Medium | Up to 100 Mbps/km | ≤10 | ≤1 000 m along rail tracks including bad weather conditions (Note 5) | ≤1 000 m along rail tracks including bad weather conditions (Note 5) |

NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.
NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.
NOTE 3: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.
NOTE 4: Estimates of maximum dimensions.
NOTE 5: Non-Line-of-Sight (NLOS) between UEs and UE to UE inside locomotives shall be supported.

**Table 5.6.6.2-1: Traffic characteristics for Train Ready for Departure communication**

# 5.7 Autonomous Train Control and Operation

## 5.7.1 Description

This section describes autonomous train control and operation in off-network mode, where no network is available. In legacy train control systems, trains typically decide its movement by interacting with trackside devices (e.g. track circuits, balise, radio block system) or communicating with a trackside server. If a train can autonomously figure out the positions of the nearby trains and decide its movement authority, the transport capacity of the railway will be enhanced. In the autonomous train control system whose service concept is aligned to the eV2X service, trains share its position by exchanging the information without any centralized server, and each train decides how far it can be authorized to move based on the position information. It is expected that main application area will be mass transportation such as subway.

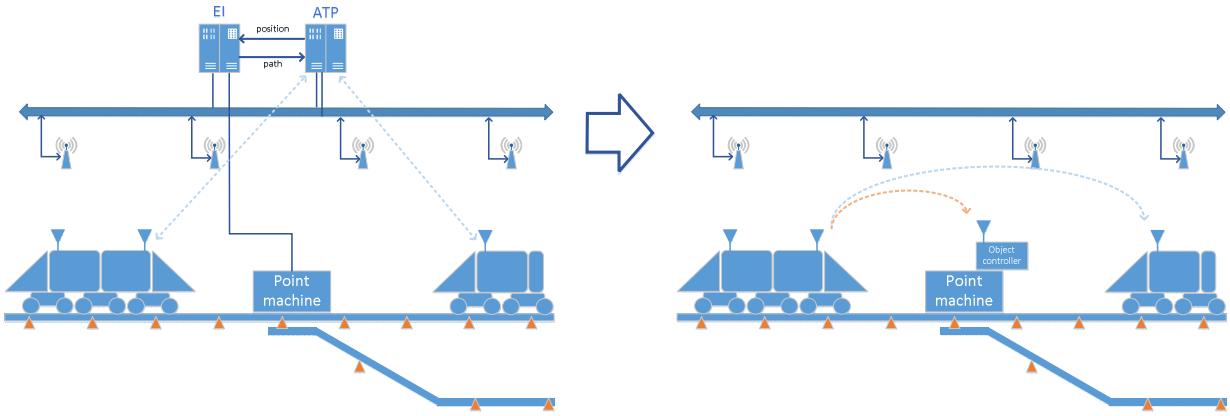



**Figure 5.7.1-1 An example of autonomous train control scenario**

## 5.7.2 Pre-conditions

1. Trains know the overall schedule, and the user equipment of each train is connected to the user equipment of the other trains operating at the same time in on-network mode. If on-network mode is not available, the user equipment is connected to the user equipment of other trains in proximity using off-network mode.

2. A user equipment of each train is able to establish a connection with the object controller for the nearby point machine, where the point machine is a trackside element.

### 5.7.3 Service Flows

1. A train gets started and try registration to the currently operating trains. As a result of the registration, every train positions are known before running.

2. The train gets the responses of the registration from the other trains and estimates the positions of the trains.

3. The train decides its movement authority based on the position information and starts moving.

4. The train positions in the corresponding areas are shared through broadcasting or multicasting. Here, the train position information is updated in a periodic manner.

5. Based on the periodically updated information, each train updates its movement authority and conduct train control based on it.

6. If the train needs to connect to the nearby point machine, the train sends switch command with a reliable mechanism in the application layer.

### 5.7.4 Post-conditions

The autonomous train control is achieved by activating movement authority for each train or activating object controller for nearby point machine.

### 5.7.5 Existing features partly or fully covering the use case functionality

The potential new requirement in the followings have been considered only in TR 22.989 V18.0.0.

### 5.7.6 Potential New Requirements needed to support the use case

#### 5.7.6.1 Requirements related to the Service layer

[PR 5.7.6.1-1] The FRMCS System shall provide a reliable mechanism to discover a FRMCS UEs in proximity in off-network.

[PR 5.7.6.1-2] The FRMCS System shall be able to share the train position periodically from one single UE to multiple FRMCS UEs in proximity for train control in off-network.

[PR 5.7.6.1-3] The FRMCS System shall be able to transmit train control data originated from one FRMCS UE to another FRMCS UE in off-network.

#### 5.7.6.2 Requirements related to the Transport layer

[PR 5.7.6.2-1] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of data transfer for direct communication for autonomous train control and operation:

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL and SL) | Payload size (Note 2) | Area traffic density (UL and DL and SL) | Overall UE density | Communication range | Service area dimension (Note 3) |
|---|---|---|---|---|---|---|---|---|---|
| Autonomous train control and operation data communication (Korea, urban railway) | ≤100 ms | 99.99 % | ≤100 km /h | ≤1 Mbps | Small to large | ≤5 Mbps/km | ≤15 (3000 m) | ≤3000 m (Note 5) | ≤3000 m along rail tracks including bad weather conditions (Note 4) |
| | NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.<br>NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.<br>NOTE 3: Estimates of maximum dimensions.<br>NOTE 4: Non-Line-of-Sight (NLOS) between UEs shall be supported.<br>NOTE 5: UEs are assumed to be located at the tail of the leading train and the front of the following train | | | | | | | | |

**Table 5.7.6.2-1: Traffic characteristics for autonomous train control and operation communication – off network communication**

Note: This table is intended to be included in Section 6.2.2.3-1 of TS 22.289 [2]

# 5.8 Virtual Coupling

## 5.8.1 Description

One of the important missions that the future railway service should achieve is to increase its transport capacity. A straight-forward solution is to minimize the distance between successive trains so that train interval is reduced. It is difficult to do so in a legacy train control system, because the successive trains need to have distance as much as a safety margin, which should be larger than the full braking distance.

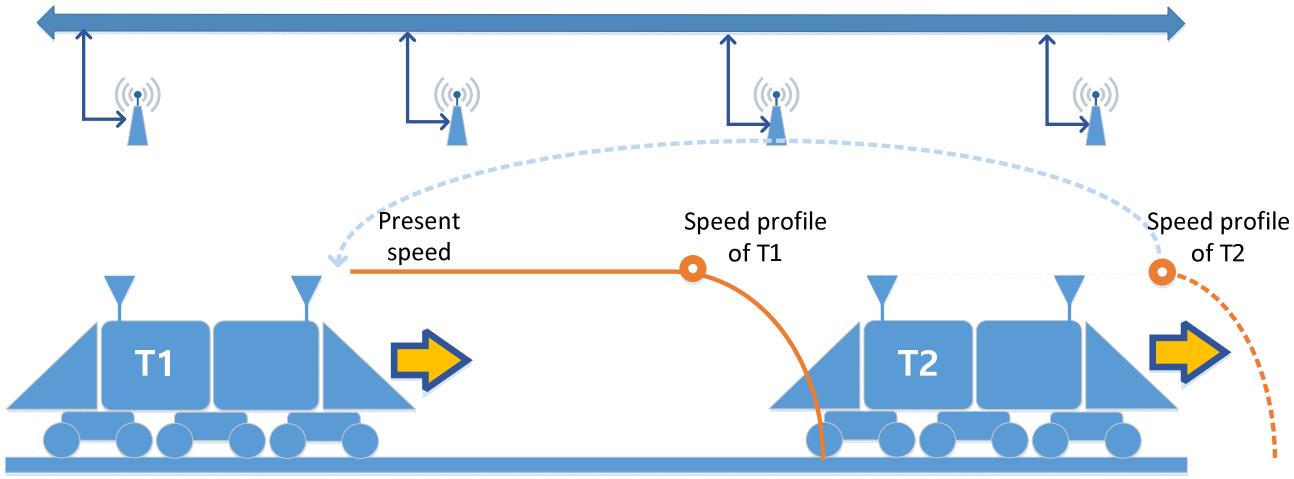



**Figure 5.8.1-2 Sharing acceleration and braking control information to shorten safety margin**

This safety margin can be further shortened if the successive trains share control information (acceleration and braking) and apply it to its own train control. As shown in Figure 5.8.1-1, the safety margin can be shortened if the following train (T1) immediately knows that the leading train (T2) starts braking and also triggers braking. This is the fundamental principle and the main purpose of virtual coupling. Figure 5.8.2 shows the basic concept of the virtual coupling scenario. Multiple trains which are in close distance move together as they are physically coupled. As the distance between two trains gets smaller, the control information of a train should be delivered to the other in shorter time.

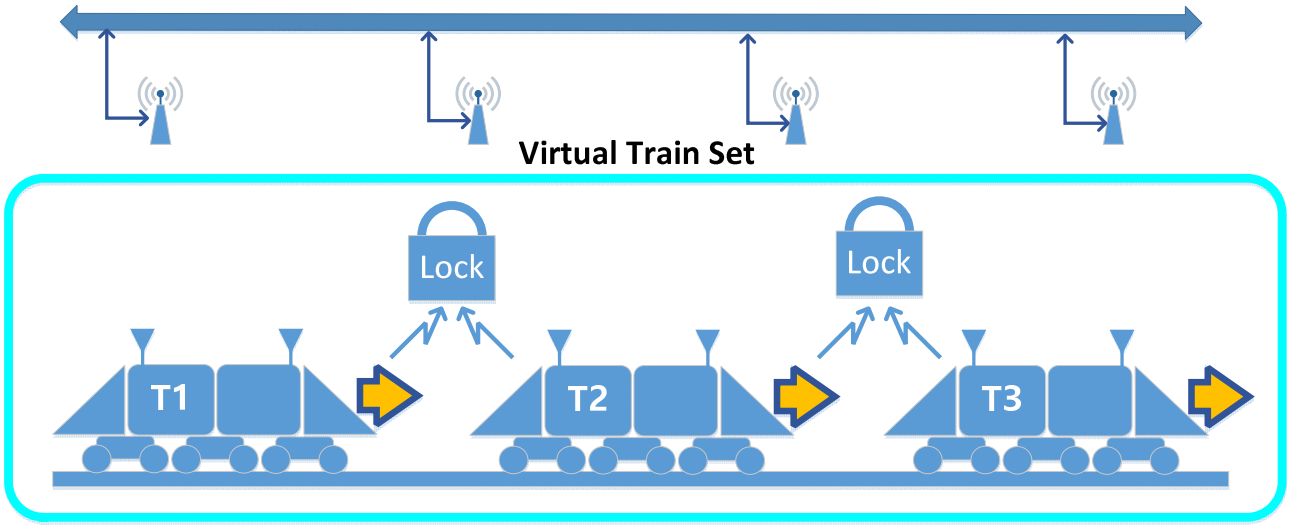



**Figure 5.8.1-2 The concept of virtual coupling scenario**

## 5.8.2 Pre-conditions

1. The leading and following trains in operation recognize each other and have just got configured to be coupled virtually. Here, the recognition is achieved by on-network or off-network.

2. The user equipments for train control support device to device communications in the perspective of transport layer.

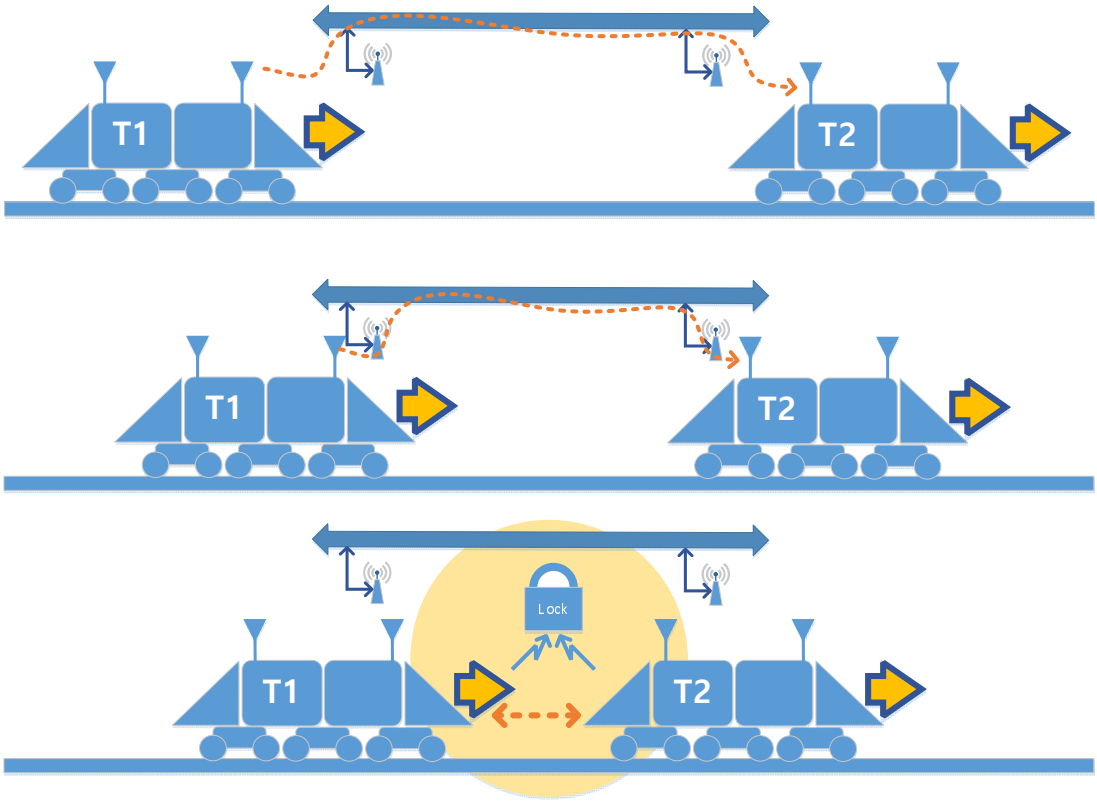



**Figure 5.8.1-3 Overall procedure of virtual coupling**

### 5.8.3 Service Flows

1. The following train begins to approach to the leading train by exchanging the information about their position. The two trains, which are far enough to allow a certain amount of end-to-end latency, are initially connected through the on-network.

2. As the following train approaches to the leading train, they start exchanging the information about movement control and each train then controls itself while considering the control of the other train. The two trains, which are still far enough to allow a certain amount of end-to-end latency, keep the connection through the on-network.

3. As the following train further approaches to the leading train, the safe braking distance gets shorter and they are required to have a connection of which end-to-end latency is very short for delicate train control. At this moment, they seamlessly switch the connection from the on-network to off-network. Each train can maintain the on-network connection, as an auxiliary connection, as long as it is within the coverage.

4. As the following train even further approaches the leading train so that the distance between the tail-end of the leading train and the front-end of the following train becomes shorter than the safe braking distance, the off-network connection requires extremely high reliability as well as short end-to-end latency to prevent potential accidents. In this case, two trains can be regarded as if they are physically coupled, communicating via wireless train backbone (WLTB).

### 5.8.4 Post-conditions

For safety train operation, integrity needs to be checked for train control information delivery in the perspective of application or transport layer. Any error on integrity check shall be immediately reported to the train control application.

### 5.8.5 Existing features partly or fully covering the use case functionality

The potential new requirement in the followings have been considered only in TR 22.989 V18.0.0.

### 5.8.6 Potential New Requirements needed to support the use case

#### 5.8.6.1 Requirements related to the Service layer

Note: Off-network is used even when network coverage is available.

[PR 5.8.6.1-1] The FRMCS system shall be able to provide integrity protection for off-network train control communication.

[PR 5.8.6.1-2] The FRMCS System shall support seamless service continuity between on-network based connection and off-network based connection

[PR 5.8.6.1-3] The FRMCS System shall support UEs capable of utilizing off-network and on-network communications at the same time.

[PR 5.8.6.1-4] The FRMCS System shall provide a mechanism to change the QoS requirements of the off-network communication adaptively.

#### 5.8.6.2 Requirements related to the Transport layer

[PR 5.8.6.2-1] The FRMCS system shall be able to provide integrity protection for off-network train control communication

[PR 5.8.6.2-2] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of data transfer for direct communication for virtual coupling:

Note: This table is intended to be included in Section 6.2.2.3-1 of TS 22.289 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | UE Relative Speed | User experienced data rate (UL and DL and SL) | Payload size (Note 2) | Area traffic density (UL and DL and SL) | Overall UE density | Communication range | Service area dimension (Note 3) |
|---|---|---|---|---|---|---|---|---|---|---|
| Virtual coupling, critical data communication (Korea, urban railway) | ≤ 100 ms | 99.99% | ≤100 km/h | ≤ 50km/h | ≤1Mbps | Small to large | ≤5 Mbps/km | ≤15 (3000 m) | ≤3000 m (Note 6) | ≤3 000 m along rail tracks including bad weather conditions |
| Virtual coupling, Very critical data communication (Korea, urban railway) (Note 5) | ≤ 10 ms | 99.9999 % | ≤100 km/h | ≤ 50km/h | ≤1Mbps | Small to large | ≤20 Mbps/km | ≤6 (300 m) | ≤ 300 m (Note 6) | ≤300 m along rail tracks including bad weather conditions (Note 4) |
| | NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.<br>NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.<br>NOTE 3: Estimates of maximum dimensions.<br>NOTE 4: Non-Line-of-Sight (NLOS) between UEs shall be supported.<br>NOTE 5: Data link between trains can work as like wireless train backbone<br>NOTE 6: UEs are assumed to be located at the tail of the leading train and the front of the following train | | | | | | | | | |

**Table 5.8.6.2-1: Traffic characteristics for Virtual coupling communication**

[PR 5.8.6.2-3] The FRMCS System shall establish an immediate communication session between entities for virtual coupling.

Editor's note: The requirement above is FFS

[PR 5.8.6.2-4] The FRMCS System shall support seamless service continuity between on-network based connection and off-network based connection.

Editor's note: The requirement above is FFS

[PR 5.8.6.2-5] The FRMCS System shall support UEs capable of utilizing off-network and on-network communications at the same time.

Editor's note: The requirement above is FFS

## 5.9 Monitoring and control of critical infrastructure communication

### 5.9.1 Description

Monitoring and controlling critical infrastructure such as train detection, signals and indicators, movable infrastructure, level crossing elements, including barrier controls, vehicle sensors, lighting controls and alarms, are essential part of operating trains in areas where no network is available e.g. rural areas, harbours.

Monitoring and controlling critical infrastructure can be done by radio, in on-network or in off-network modes. This section describes monitoring and control of critical infrastructure communications in off-network mode, where no network is available. No service handover between on-network and off-network modes is foreseen.

## 5.9.2 Pre-conditions

The Chief conductor (i.e. the FRMCS User) is authorised to initiate Monitoring or controlling critical infrastructure communications.

## 5.9.3 Service Flows

Monday, 9:30 in the morning. James has been assigned the role of the lead driver of train #12345. His train #12345 stands in platform A, located in a Harbour railway station where there is no network coverage. The train is ready for boarding and starts running at 10:00. James is located in the front cabin (indoor).

Before leaving the Harbour area, James has to run its train through many level crossings. In order to run safely the level crossing (LX), James has to detect vehicles in the level crossing area using fixed video camera of this area.

James is equipped with an onboard device with display connected to a UE. LX surveillance camera is also connected to a UE. James and the camera are operating their UEs in off-network mode and have selected their role to enable video exchanges. The video communications are encrypted to prevent eavesdropping.

When James approaching the LX, James enables video from LX surveillance camera to detect vehicles. James primarily relies on the remote LX surveillance camera vision to identify obstacles (e.g. vehicles) and to make decision on whether to enter the LX area. When no vehicles are detected, James is allowed to run its train through the LX area. When the train has left the LX area, James disable videos from LX surveillance camera. James continues running his train to next LX.

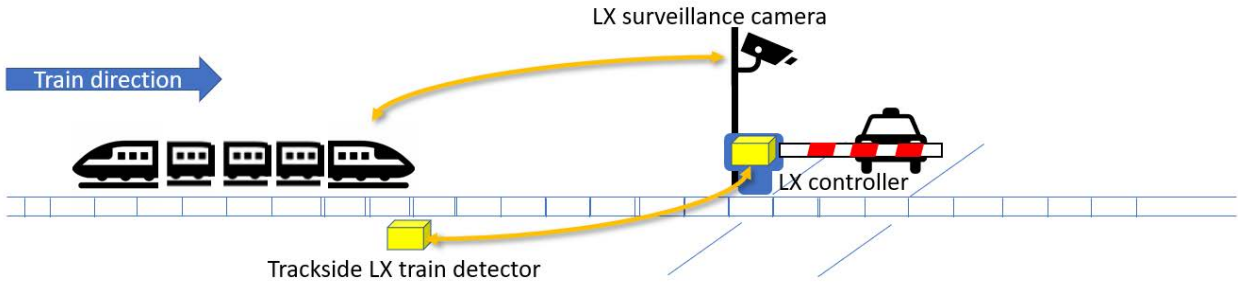



**Figure 5.9.3-1: Monitoring and control of critical infrastructure communications**

## 5.9.4 Post-conditions

Monitoring and controlling critical infrastructure videos are safely exchanged between the Chief Conductor and the Fixed Cameras to avoid any safety related issue at level crossings.

## 5.9.5 Existing features partly or fully covering the use case functionality

TS 22.280 [4], 22.179 [3], 22.281 [5] and 22.282 [6] have a set of specific requirements on Off-Network MCX Services (including MCCoRe and MCData Services for Off-Network).

TS 22.289 [2] has a set of performance requirements for Off-Network communications for Rail to be refined based on outcomes of the present study.

TS 22.261 [7] has no requirement on 5G Proximity Services.

TS 22.185 [8] and 22.186 [9] have a set of specific requirements on 5G Proximity Services to support V2X communications.

## 5.9.6 Potential New Requirements needed to support the use case

### 5.9.6.1 Requirements related to the Service layer

[PR 5.9.6.1-1] The FRMCS Service in Off-Network mode shall be able to initiate video communications for Monitoring and controlling critical infrastructure to relevant FRMCS User upon a request from a functional identity entitled to initiate such communication.

[PR 5.9.6.1-2] The FRMCS Service in Off-Network mode shall provide the necessary communication means to support Monitoring and controlling critical infrastructure.

[PR 5.9.6.1-3] The FRMCS Service in Off-Network mode shall allow arbitration for Monitoring and controlling critical infrastructure.

[PR 5.9.6.1-4] The FRMCS Service in Off-Network mode shall be able to terminate video communications for Monitoring and controlling critical infrastructure upon a request received from a functional identity entitled to terminate such communication.

[PR 5.9.6.1-5] The FRMCS Service in Off-Network mode shall provide the means to record Monitoring and controlling critical infrastructure communication and communication related information (e.g. FRMCS Users involved and their roles) to an external system.

[PR 5.9.6.1-6] The FRMCS Service Security Framework shall provide mechanisms in Off-Network mode to cover identity management, authentication, authorisation and data protection in respect to Monitoring and controlling critical infrastructure.

### 5.9.6.2 Requirements related to the Transport layer

[PR 5.9.6.2-1] The FRMCS Service in Off-Network mode shall support the following traffic characteristics of video transfer for direct communication for Monitoring and controlling critical infrastructure:

Note: this table is intended to be aligned with TS 22.289 table 5.2.2-2 [2]

| Scenario | End-to-end latency | Reliability (Note 1) | UE speed | User experienced data rate (UL and DL) | Payload size (Note 2) | Area traffic density (UL and DL) | Overall UE density | Communication range (Note 3) | Service area dimension (Note 4) |
|---|---|---|---|---|---|---|---|---|---|
| Monitoring and controlling critical infrastructure video Communication | ≤100 ms | 99,9% | ≤40 km/h | 10 Mbps | Medium | Up to 20 Mbps/km | 2 | ≤1 000 m along rail tracks including bad weather conditions (Note 5) | ≤1 000 m along rail tracks including bad weather conditions (Note 5) |
| | NOTE 1: Reliability as defined in TS 22.289 sub-clause 3.1.<br>NOTE 2: Small: payload ≤ 256 octets, Medium: payload ≤512 octets; Large: payload 513 -1500 octets.<br>NOTE 3: Supported via a single or a combination of 3GPP capabilities of 5GS that best serve these use case in areas with no FRMCS RAN nodes/no FRMCS network coverage.<br>NOTE 4: Estimates of maximum dimensions.<br>NOTE 5: Non-Line-of-Sight (NLOS) between UEs and UE to UE inside locomotives shall be supported. | | | | | | | | |

**Table 5.9.6.2-1: Traffic characteristics for Monitoring and controlling critical infrastructure communication**

# 6 Void.

## 6.1 Void.

# 7 Void.

## 7.1 Void.

# 8 Identified issues

## 8.1 Introduction

This section summarizes open points identified by SA1 as part of the gap analysis of the use cases captured above, e.g. about limitations, missing requirements and gaps in existing functionalities supported by 3GPP.

## 8.2 Identified issue 1: Communication range

### 8.2.1 Description

Some of the use cases described in clauses 5, 6 and 7 of the present document (e.g. the Trackside Maintenance Warning System communication) require communication range of up to several kilometres (e.g. 8.5 km) along rail tracks including tunnels, bad weather conditions, unfavourable geographical conditions, and non-Line-of-Sight (NLOS) between UEs i.e. obstructions.

Communication range is to be understood as the maximum distance between users operating UEs without performance degradations. Users may be stationary, pedestrians or in motion up to 500 kmph.

### 8.2.2 Limitations, missing requirements and gaps

<Describe limitations, missing requirements and gaps in existing functionalities supported by 3GPP, identified during this study.>

## 8.3 Identified issue 2: MCX Support

### 8.x.1 Description

Some of the use cases described in clauses 5, 6 and 7 of the present document (refer to subclauses describing requirements to the Service layer) require support of MCX Services.

The following MCX capabilities should be supported by Off-Network for Rail.

Due to the nature of Off-Network communication, it is expected that the functionality of those MCX capabilities might be reduced compared to On-Network communication.

- MCX Service common capabilities:
    - Group communications,
    - Private communications,
    - Late Communication Entry,

- Functional Alias,
- Location Service,
- E2E Security,
- User Authentication and Service Authorization,
- Service Arbitration,
- QoS and Priority,
- Performance Monitoring and Exposure Service,
- Recording Metadata,
- Transition from Off-Network to On-Network (and vice-versa) (i.e. Service Continuity),
- Service Configuration (i.e. local + central when transiting from Off-Network to On-Network),

- MCX Service Types:
  - MCPTT,
  - MCData,
  - MCVideo.
- MCX Service capabilities per Service Type:
  - MCPTT
    - Floor Control,
    - Multi-Talker Control.
  - MCData
    - SDS,
    - IP Connectivity.
  - MCVideo
    - Video Streams.

### 8.x.2 Limitations, missing requirements and gaps

<Describe limitations, missing requirements and gaps in existing functionalities supported by 3GPP, identified during this study.>

## 8.x Identified issue y: <Identified issue title>

### 8.x.1 Description

<Describe the issue (i.e. problem statement).>

### 8.x.2 Limitations, missing requirements and gaps

<Describe limitations, missing requirements and gaps in existing functionalities supported by 3GPP, identified during this study.>

# 9 Consolidated potential requirements

# 10 Conclusion and recommendations

This technical report identifies several use cases, and potential new requirements for 5GS support of Rail Off-Network. Some open points identified as part of the gap analysis of the use cases have been collected and detailed in clause 8 (e.g., communication range, MCX support).

A further step is necessary to identify limitations, missing requirements and gaps in existing functionalities supported by 3GPP before any potential normative work. This step could be performed by external bodies involved in the definition of Rail Off-Network use cases (e.g., UIC, ETSI TC RT).

It is therefore recommended to wait for further gap analysis before finalizing consolidated requirements in this TR and trigger potential subsequent normative work (if deemed necessary).

# Annex A:
# Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-09 | SA1#91-e | S1-203281 | | | | TR Skeleton for Study on Off-Network for Rail | 0.0.0 |
| 2020-09 | SA1#91-e | S1-203254 | | | | FS_OFFNETRAIL TR 22.990 Introduction | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203355 | | | | FS_OFFNETRAIL TR 22.990 Scope | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203256 | | | | FS_OFFNETRAIL TR 22.990 Overview | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203257 | | | | FS_OFFNETRAIL TR 22.990 Chapter 5 | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203258 | | | | FS_OFFNETRAIL TR 22.990 Chapter 6 | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203259 | | | | FS_OFFNETRAIL TR 22.990 Chapter 7 | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203328 | | | | FS_OFFNETRAIL TR 22.990 Key Issues | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203329 | | | | FS_OFFNETRAIL TR 22.990 UC Trackside Maintenance Warning System | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203330 | | | | FS_OFFNETRAIL TR 22.990 UC Remote Control of Engines | 0.1.0 |
| 2020-09 | SA1#91-e | S1-203385 | | | | Incorporated all agreed contributions to TR 22.990 at SA1#91e | 0.1.0 |
| 2020-11 | SA1#92-e | S1-204035 | | | | Introduce “Train integrity monitoring data communication” use case | 0.2.0 |
| 2020-11 | SA1#92-e | S1-204036 | | | | Introduce “Shunting communication” use case | 0.2.0 |
| 2020-11 | SA1#92-e | S1-204037 | | | | Introduce “Train ready for departure communication” use case | 0.2.0 |
| 2020-11 | SA1#92-e | S1-204413 | | | | Autonomous Train Control and Operation: Moving Authority Perspective | 0.2.0 |
| 2020-11 | SA1#92-e | S1-204414 | | | | Virtual Coupling Use Case | 0.2.0 |
| 2020-11 | SA1#92-e | S1-204148 | | | | Identified issue: Communication range | 0.2.0 |
| 2021-03 | SA1#93-e | S1-210228 | | | | Enhance “Train ready for departure communication” use case with video | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210230 | | | | Enhance “Shunting communication” use case with video | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210427 | | | | New “Monitoring and Control of Critical Infrastructure communication” use case | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210428 | | | | Off-Net Railways_Update to sec.8 | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210429 | | | | Add “MCX Support” as an identified issue to be solved by 3GPP technology as required by Off-Network for Rail | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210430 | | | | Enhancement of “Virtual coupling” use case | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210240 | | | | Do not exclude any single or a combination of 3GPP capabilities to support Rail Off-Network use cases | 0.3.0 |
| 2021-03 | SA1#93-e | S1-210244 | | | | Request for clarification on relationship between TR 22.990 and TS 22.289 QoS scenarios and traffic characteristics | 0.3.0 |
| 2021-09 | SA1#95-e | S1-213292 | | | | Updates to “Virtual coupling” use case | 0.4.0 |
| 2021-09 | SA1#95-e | S1-213293 | | | | Updates to “Autonomous train control and operation” use case | 0.4.0 |
| 2021-09 | SA1#95-e | S1-213294 | | | | Updates to “Conclusion and Recommendations” clause | 0.4.0 |
| 2021-09 | SA#93e | SP-211043 | | | | Raised to v.1.0.0 for presentation for information | 1.0.0 |
| 2021-11 | SA1#96-e | S1-214031 | | | | Global clean up to remove unnecessary clauses | 1.1.0 |
| 2021-11 | SA1#96-e | S1-214032 | | | | Clean up of references | 1.1.0 |
| 2021-12 | SA#94e | SP-211504 | | | | Raised to v.2.0.0 for presentation for approval | 2.0.0 |
| 2021-12 | SA#94e | SP-211504 | | | | Raised to v.18.0.0 following SA#94e's approval | 18.0.0 |
| 2025-10 | SA#109 | - | - | - | - | Updated to Rel-19 by MCC | 19.0.0 |

# History

| Document history | | |
|---|---|---|
| V19.0.0 | October 2025 | Publication |
| | | |
| | | |
| | | |
| | | |