ETSI Plugtests Report V1.0.0 (2022-06)

2nd ETSI FRMCS Plugtests
Remote Event
16 – 20 May 2022

Keywords
Testing, Interoperability, Mission-Critical, LTE,
MCPTT. MCX, FRMCS

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-préfecture de Grasse (06) N° 7803/88

Contents

Executive Summary

The Future Rail Mobile Communications System (FRMCS) is using for its specific features the MCX (collectively for MCPTT, MCVideo and MCData services) framework. This was tested during the 2nd FRMCS Plugtests from 16th May to 20th May 2022 remotely. 60 test sessions were executed between vendors, based on 3GPP Release-17.

The 2nd ETSI FRMCS Plugtests have concluded with a success rate of 95% of the executed tests in the validation of 3GPP mission critical services vendor interoperability.

These tests are essential to ensure seamless access to mission critical services across different vendors' products and implementations.

The MCX ETSI Plugtests series is the first independent testing of public safety and other mission critical LTE. The MCX services are the basis for the Future Rail Mobile Communications System (FRMCS). The preparations for the 2nd FRMCS Plugtests started in February 2022 and were concluded by a remote testing week in May 2022.

The tests were based on 3GPP Release-17 and 338 tests were executed between the different vendors in 60 test sessions. The MCX Plugtests test specification has been amended with additional rail specific test scenarios and will be included in a future version of ETSI TS 103 564 (after the ETSI committee TCCE approval).

Additionally, five observations were gathered during the Plugtests event preparation and testing. The observations from the Plugtests events provide essential feedback to 3GPP Working Groups as work continues on mission critical communication specifications.

This 2nd FRMCS Plugtests was organized by ETSI with the support of the European Commission, EFTA, TCCA and UIC.

The Plugtests event was a pure interoperability testing event and no products were certified.

The next MCX#7 Plugtests event is planned for 07 - 11 November 2022 at the University of Malaga in Spain.

The following equipment was provided by the companies participating in this FRMCS Plugtests:

FRMCS MCX Application Servers:

- Alea
- Consort Digital
- Kontron
- Leonardo
- MCLabs
- Nemergent Solutions
- Nokia
- TASSTA

FRMCS MCX Clients:

- Alea
- Consort Digital
- Frequentis
- Funkwerk
- Kontron
- Leonardo
- Nemergent Solutions
- Siemens
- Softil
- TASSTA
- Teltronic

Evolved Packet Core:

- Athonet

User Equipment:

- Leonardo
- Teltronic

Evolved Multimedia Broadcast Multicast Services (eMBMS) Components:

- Athonet

Test Tool Vendors:

- Viavi Solutions
- Valid8


PLUGTESTS Vendors
ALEA a LEONARDO company
ATHONET
FREQUENTIS
funkwerk
mclabs
VIAVI Solutions
CONSORT
kontron
nemergent solutions
SIEMENS
LEONARDO
NOKIA
VALID8.com
SOFTIL INNOVATIVE COMMUNICATIONS
TASSTA
teltronic
PLUGTESTS Observers
astrid
DB
Home Office
ŽSR
SNCF RÉSEAU
STRATIVIA
TCCA
uic
ERILLISVERKOT
*Endorsed by NIST
RAIL SYSTEMS AUSTRALIA
Grundy County ETSB 911 Emergency Telephone System Board
Rail Baltic Estonia
VICTORIA State Government Department of Transport
smit
Transport Sydney Trains

1 Introduction

Mission Critical MCX Services (MCPTT, MCVideo and MCData) are standardized services which ensure that LTE and 5G systems support mission-critical communications. The Future Rail Mobile Communications System (FRMCS) is based on these MCX services.

The Global Mission-Critical Communication Market was valued at USD 13.63 Billion in 2018 and is estimated to reach USD 26.66 Billion by 2025 growing at a CAGR of 10.5% during the forecast period 2019–2025, according to the market research. The first nationwide rollouts in the United States, South Korea, the UK, the Middle East and Asian countries are expected to trigger significant large-scale investments in mission-critical LTE.

Mission Critical Push To Talk (MCPTT) was the first of a number of Mission Critical features which was introduced by 3GPP in Release-13. Mission Critical Video (MCVideo) and Mission Critical Data (MCData) were introduced in Release-14. With the standardization of MCX (Mission-Critical PTT, Video & Data), IOPS (Isolated Operation for Public Safety), and other critical communications features by 3GPP, LTE and 5G networks are increasingly gaining recognition as an all-inclusive communications platform for public safety, rail and other critical communications sectors.

Preparations for the 2nd ETSI FRMCS Plugtests event started in February 2022 with the registrations of vendors and observers. During bi-weekly conference calls from February to May 2022 the setup of the tests, the test specification and organizational issues were agreed between the participants. Before the main event, the vendors have been done remote pre-testing of their implementations via VPN tunnels which connected their labs to a central exchange hub.

All the information required to organise and manage the 2nd FRMCS Plugtests event was compiled and shared with participants in a dedicated private WIKI which was put in place by ETSI. All participants were provided with credentials that allowed them to access and update their details. All the information presented in this document has been extracted from the 2nd FRMCS Plugtests event wiki: https://wiki.plugtests.net/2nd-FRMCS-Plugtests/index.php?title=Main_Page (login required). Clause 4 describes the management of the Plugtests event.

The following equipment was tested – please see also clause 5:

- FRMCS MCX Application Servers (FRMCS MCX AS)
- FRMCS MCX Clients
- User Equipment (UE)
- Test Tools

This Plugtests specifically focused on railways-oriented features of the Application Servers and Clients.

A dedicated Test Tools test stream was available for test tool vendors and other vendors to check their tools and the conformance of their implementations with a test tool.

The remote test infrastructure is described in clause 6; the test procedures are described in clause 7.

The vendors and ETSI have set up VPN-Tunnels from the vendors' premises to the ETSI VPN hub. This allowed the vendors to start integration work and pre-testing of MCX services.

For the 2nd FRMCS Plugtests additional 14 test cases were developed by ETSI. An updated version of the test specification, including the new FRMCS test cases, will be published as a new version of ETSI document ETSI TS 103 564 (after ETSI TC TCCE approval).

About 338 tests were conducted by the vendors. 95% of the tests were successful, the remaining 5% failed for various reasons. The detailed results of the tests are available for the involved vendors in these test sessions but are not disclosed to the other vendors or to the public. All participants had to sign a Non-Disclosure Agreement and Rules of Engagement before joining the Plugtests event. The statistics of the test results are listed in clause 9.

The failed tests give the vendors valuable information to improve their implementations. They also help to discover ambiguities in the 3GPP standards and to clarify and improve the specifications.

ETSI plan to conduct more FRMCS and MCX Plugtests in the future. The next MCX Plugtests sessions are planned for November 2022. Vendors who have participated in past MCX Plugtests, and vendors which have not participated in the previous MCX or FRMCS Plugtests events are welcomed and encouraged to join the next MCX Plugtests event planned for November 2022.

2 References

The following documents have been used as references in the Plugtests. The participants in the Plugtests agreed on a set of specific documents and **Release 17 Technical Specifications (versions available in March 2022)** for the second FRMCS Plugtests. Please see also the test specification document for the references.

[1] ETSI TS 103 564: Plugtests scenarios for Mission Critical Services.

[2] 3GPP TS 22.179: Mission Critical Push to Talk (MCPTT) over LTE.

[3] 3GPP TS 23.280: Common functional architecture to support mission critical services.

[4] 3GPP TS 23.379: Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT).

[5] 3GPP TS 24.229: IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

[6] 3GPP TS 24.281: Mission Critical Video (MCVideo) signalling control; Protocol specification.

[7] 3GPP TS 24.282: Mission Critical Data (MCData) signalling control.

[8] 3GPP TS 24.379: Mission Critical Push To Talk (MCPTT) call control.

[9] 3GPP TS 24.380: Mission Critical Push To Talk (MCPTT) media plane control.

[10] 3GPP TS 24.481: Mission Critical Services (MCS) group management.

[11] 3GPP TS 24.482: Mission Critical Services (MCS) identity management.

[12] 3GPP TS 24.483: Mission Critical Services (MCS) Management Object (MO).

[13] 3GPP TS 24.484: Mission Critical Services (MCS) configuration management.

[14] 3GPP TS 24.581: Mission Critical Video (MCVideo) media plane control.

[15] 3GPP TS 24.582: Mission Critical Data (MCData) media plane control.

[16] 3GPP TS 26.179: Mission Critical Push To Talk (MCPTT); Codecs and media handling.

[17] 3GPP TS 26.346: Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs.

[18] 3GPP TS 29.212: Policy and Charging Control (PCC); Reference points.

[19] 3GPP TS 29.214: Policy and Charging Control over Rx reference point.

[20] 3GPP TS 29.468: Group Communication System Enablers for LTE (GCSE_LTE); MB2 reference point.

[21] 3GPP TS 33.180: Security of the mission critical service.

[22] IETF RFC 3515: The Session Initiation Protocol (SIP) Refer Method.

[23] IETF RFC 3856: A Presence Event Package for the Session Initiation Protocol (SIP).

[24] IETF RFC 3903: Session Initiation Protocol (SIP) Extension or Event State Publication.

[25] IETF RFC 4488: Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription.

[26] IETF RFC 4825: The Extensible Markup Language (XML) Configuration Access Protocol (XCAP).

[27] IETF RFC 5366: Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP).

[28] IETF RFC 5373: Requesting Answering Modes for the Session Initiation Protocol (SIP).

[29] IETF RFC 5875: An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package.

[30] IETF RFC 6135: An Alternative Connection Model for the Message Session Relay Protocol (MSRP).

[31] IETF RFC 6665: SIP-Specific Event Notification.

[32] IETF RFC 7647: Clarifications for the use of REFER with RFC6665.

[33] OMA. OMA-TS-XDM_Core-V2_1-20120403-A: XML Document Management (XDM) Specification.

[34] OMA. OMA-TS-XDM_Group-V1_1_1-20170124-A: Group XDM Specification.

[35] IETF RFC 7230: Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing..

[36] IETF RFC 5246: The Transport Layer Security (TLS).

[37] IETF RFC 6101: The Secure Sockets Layer (SSL).

[38] IETF RFC 4975: The Message Session Relay Protocol (MSRP).

[39] 3GPP TR 21.905: Vocabulary for 3GPP Specifications

3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [39] 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 [39].

AMR	Adaptative Multi-Rate Audio Codec
AMR-WB	Adaptative Multi-Rate Audio Codec Wideband
APP	Application
AS	Application Server
CMS	Configuration Management Server
CSC	Common Services Core
CSCF	Call Session Control Function
CSK	Client-Server Key
DUT	Device Under Test
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETSI	European Telecommunications Standard Institute
EUT	Equipment Under Test
FD	File Distribution
FA	Functional Alias
FE	Functional Element
FRMCS	Future Railway Mobile Communication System
GCSE	Group Communication Service Enabler
GMK	Group Master Key
GMS	Group Management Server
iFC	Initial Filter Criteria
IFS	Interoperable Functions Statement
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IdMS	Identity Management Server
KMS	Key Management Server
MBMS	Multimedia Broadcast and Multicast Service
MCData	Mission Critical Data
MCPTT ID	MCPTT user identity
MCPTT	Mission Critical Push-To-Talk
MCVideo	Mission Critical Video
MCX	Mission Critical Services (X stands for PTT, Data and Video)
OAM	Operation and Maintenance
OTT	Over the Top
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
PES	Pre-established Sessions
PSI	Public Service Identity
PSTA	Public Safety Technology Association
PTT	Push-To-Talk
ProSe	Proximity-based Services
RAN	Radio Access Network
RTP	Real-time Transport Protocol
SDS	Short Data Service
SIP	Session Initiation Protocol
SPK	Signalling Protection Key
TCCA	The Critical Communications Association
TD	Test Description
TR	Technical Recommendation
TRT	Test Reporting Tool
TS	Technical Specification
UE	User Equipment

UIC	International union of railways (Union Internationale des Chemins de fer)

4 Technical and Project Management

4.1 Scope

The main goal of the 2nd FRMCS Plugtests was testing the interoperability of the MCPTT, MCData and MCVideo ecosystem signalling and media plane at different levels. The railway related functionalities were the focus of the interoperability event.

The basic scenario in FRMCS Plugtests comprises FRMCS MCX application server(s) - both controlling and participating - and FRMCS MCX clients deployed over a generic SIP/IMS core and UEs. The following figure (Fig 1) illustrates the basic test infrastructure. In this 2nd FRMCS Plugtests most of the tests were carried out Over-The-Top (OTT) using pure IP connectivity and FRMCS features on top of the MCX components were specially considered.

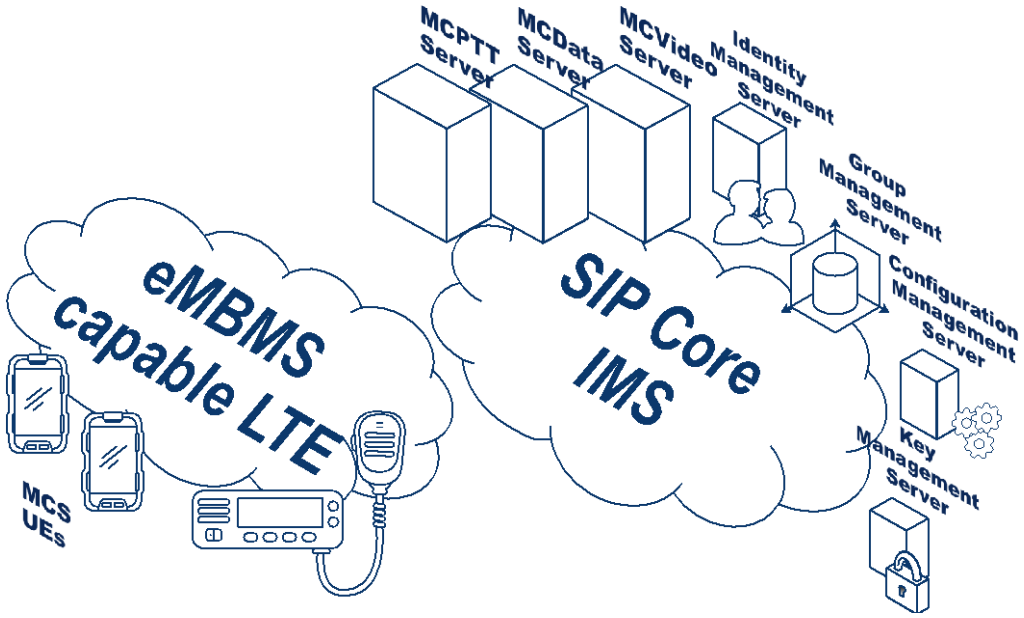


Figure 1. Typical MCPTT/MCData/MCVideo scenario to be considered in the Plugtests

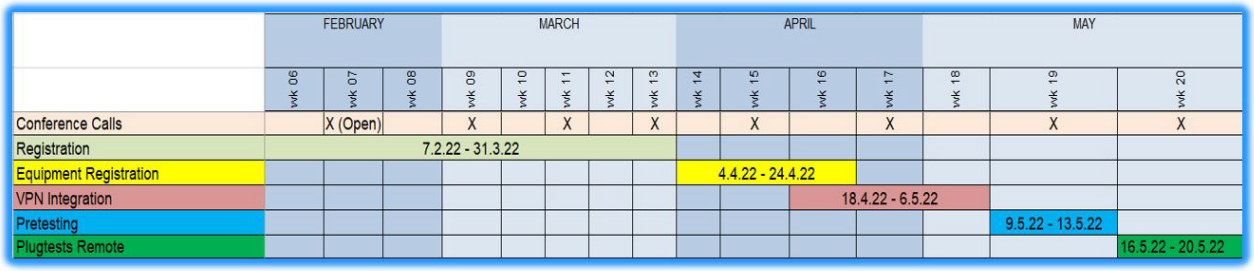
In the scope of this Plugtests event, the following high-level test objectives were performed

- **Connectivity (CONN):** MCPTT call forwarding, transfer and remote initiation.
- **Floor Controlling (FC):** Multi-talker functionality in Floor Control operations.
- **Registration and authorization (REGAUTH)**: Comprised MCX Client registration.
- **Affiliation (AFFIL)**: Affiliation change triggered by Functional Alias activation/deactivation
- **Functional alias (FA):** Apart from affiliation change, exchange of FA during call signalling and floor control, location sharing was also evaluated.
- **MCData IP Connectivity**: MCData client establishes an IP Connectivity session.
- **User/Group Regrouping:** MCPTT user requests/remove the user/group regroup.
- **MCData Message Store:** Including new notification mechanisms.
- **FRMCS scenarios:** Railways emergency communications handling.
- **Observers Test Scenarios**: Complex scenarios comprising different simpler test cases.

4.2 Timeline

The preparation was run through different phases as described in the figure below.

Schedule



	FEBRUARY			MARCH					APRIL				MAY		
	wk 06	wk 07	wk 08	wk 09	wk 10	wk 11	wk 12	wk 13	wk 14	wk 15	wk 16	wk 17	wk 18	wk 19	wk 20
Conference Calls		X (Open)		X		X		X		X		X		X	X
Registration	7.2.22 - 31.3.22														
Equipment Registration									4.4.22 - 24.4.22						
VPN Integration											18.4.22 - 6.5.22				
Pretesting														9.5.22 - 13.5.22	
Plugtests Remote															16.5.22 - 20.5.22

Figure 2. Plugtests event timeline

Registration to the FRMCS Plugtests event was open from 07th February 2022 to 31st March 2022 to any organisation willing to participate in testing the FRMCS Ecosystem. A total of 60 people was finally involved in the remote Plugtests event.

The following clauses describe the different phases of the Plugtests event preparation. It is worth noting that since the start of the documentation phase until the first week of the Plugtests event, bi-weekly conference calls were run among organisers and participants to discuss and track the progress, anticipate and solve technical issues, review the test plan, etc.

4.2.1 Documentation

Once the registration to the Plugtests event was closed, the following documentation activities were launched in parallel:

1) Equipment Under Test (EUT) Documentation

Participants documented their EUTs, by providing the information directly to the Plugtests event team. The Plugtests event team compiled the final EUT table for all the participating vendors and was appended to the Plugtests event Test Plan,

All the information described above was made available in the Plugtests event WIKI, so that it could be easily maintained and consumed by participants.

2) Test Plan Development

The Test Plan development was led by ETSI Centre for Testing and Interoperability following the methodology defined by 3GPP TSG SA6 and 3GPP TSG CT1. The Test Plan was scoped around 3GPP Test Specifications Release-16 capabilities and concentrated on the features supported by the implementations attending the Plugtests event.

The Test Plan was developed and consolidated in an iterative way, taking into account input and feedback received from Plugtests event participants. See details in clause 8.

4.2.2 Remote integration & pre-testing

Participants connected their implementations remotely to the Plugtests event infrastructure, known as HIVE: Hub for Interoperability and Validation at ETSI.

During this phase, up to 16 remote labs connected to HIVE for the FRMCS Plugtests and each of them was allocated a dedicated network. The interconnection of remote labs allowed running integration and pre-testing tasks remotely among any combination of participating EUTs, in order to ensure an efficient use of the Plugtests event time and smoother Interoperability test sessions.

A VPN connection to HIVE was highly recommended for participants providing FRMCS MCX Application Servers and FRMCS MCX Clients for first connectivity tests, trouble shooting and infrastructure access purposes.

Additional details on the remote test infrastructure, remote integration and pre-testing procedures are provided in Clauses 6 and 7.

During this phase, the bi-weekly conference calls were continued among organisers and participants to synchronise, track progress and get ready for the on-site phase.

4.2.3 Plugtests event

From 16th of May to the 20th of May 2022, participants connected their equipment with ETSI HIVE infrastructure to collaboratively run the Interoperability Test Sessions scheduled by ETSI CTI.

The 5 days were dedicated to remote interoperability test sessions involving all the participating EUTs organised in several parallel tracks, see details in Clause 4.3.2.

The scheduling of individual test combinations was done randomly using ETSI Test Reporting tool with the inputs and requests from the participants. The schedule was adapted during the test session slots on a per need basis.

4.3 Tools

4.3.1 Plugtests event WIKI

The Plugtests event WIKI was the main source of information for the FRMCS Plugtests event, from logistics aspects to testing procedures. Access to the WIKI was restricted to participating companies.

The main technical information provided in the wiki was organised as follows:

- **Event Information** – Logistics aspects of the Plugtests event.
- **Participants** – List of participants in the event.
- **Schedule**- Planning of different phases of the event.
- **Observer Program** – Information about the Observer interoperability demo during the Plugtests event.
- **Test Tools** – Information from the Test Tool vendors about what kind of tests they are offering for the Plugtests.
- **Testing Infrastructure (Network Information)** - HIVE connection request tool, and remote connections status overview.
- **Specifications -** Test specification developed during the FRMCS Plugtests.
- **Equipment Under Test** - Participating EUTs overview with feature support, test case support, integration and contact information.
- **Provisioning Information -** Pre-configured parameters for EUTs recommended and IP addresses of EUTs.
- **Test Reporting Tool** - Documentation of the Test Reporting Tool.
- **Conference Calls** - Calendar, logistics, agendas and minutes of the bi-weekly conference calls run during the remote integration and pre-testing phase.
- **Observations** - Issues found during Plugtests event.

In addition, Slack was used among the participants to communicate with each other during the pre-testing phase and Test Sessions, include their remote colleagues (back-office support) in the discussions.

4.3.2 Test Reporting Tool (TRT)

The Test Reporting Tool guides participants through the Test Plan test cases during the pre-testing and main Test Sessions. It allows creating Test Session Reports compiling detailed results for the individual scheduled Test Sessions.

Only the companies providing the EUTs for each specific Test Session combination have access to their Test Session Reports contents and specific results. All companies involved in a specific session and who have entered the test results

were required to verify and approve the reported results at the end of each session. Only test report which has been approved by all involved parties are considered as valid.

Another interesting feature of this tool is the ability to generate real-time stats (aggregated data) of the reported results, per test case, test group, test session or overall results. These stats are available to all participants and organisers and allow tracking the progress of the testing with different levels of granularity, which is extremely useful to analyse the results.

5619	2022-05-17 09:00	120	I	CFG-FRMCS-OTT	Alea - FRMCS MCX AS Leonardo - FRMCS MCX Client
5620	2022-05-18 14:00	120	IV	CFG-FRMCS-OTT	Kontron - FRMCS MCX AS Funkwerk - FRMCS MCX Client
5621	Freestyle			CFG-FRMCS-OTT	Leonardo - FRMCS MCX AS Alea - FRMCS MCX Client
5622	2022-05-19 09:00	120	IV	CFG-FRMCS-OTT	Nemergent - FRMCS MCX AS Softil - FRMCS MCX Client
5623	2022-05-18 14:00	120	I	CFG-FRMCS-OTT	Tassta - FRMCS MCX AS Softil - FRMCS MCX Client
5624	2022-05-20 09:00	120	IV	CFG-FRMCS-WIFI	Nokia - FRMCS MCX AS Softil - FRMCS MCX Client Teltronic - UE
5625	2022-05-20 16:00	120	I	CFG-FRMCS-OTT	Kontron - FRMCS MCX AS Alea - FRMCS MCX Client
5626	2022-05-16 11:00	120	II	CFG-FRMCS-OTT	Nemergent - FRMCS MCX AS ConsortDigital - FRMCS MCX Client
5627	2022-05-16 09:00	120	III	CFG-FRMCS-OTT	Alea - FRMCS MCX AS Frequentis - FRMCS MCX Client

Figure 3. Test Reporting Tool – example screen shot

5 Equipment Under Test

The tables below summarise the different EUTs provided by the Plugtests event participants:

5.1 FRMCS MCX Application Servers

Organisation	Support
Alea	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA
Kontron	MCPTT, MCDATA
Leonardo	MCPTT, MCDATA, MCVIDEO
MCLabs	MCPTT, MCVIDEO
Nemergent	MCPTT, MCDATA, MCVIDEO
Nokia	MCPTT, MCDATA, MCVIDEO
TASSTA	MCPTT, MCDATA, MCVIDEO

Table 1. FRMCS MCX Application Servers Under Test

5.2 FRMCS MCX Clients

Organisation	Support
Alea	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA
Frequentis	MCPTT, MCDATA, MCVIDEO
Funkwerk	MCPTT, MCDATA
Kontron	MCPTT, MCDATA
Leonardo	MCPTT, MCDATA, MCVIDEO
Nemergent	MCPTT, MCDATA, MCVIDEO
Siemens	MCPTT
Softil	MCPTT, MCDATA, MCVIDEO
TASSTA	MCPTT, MCDATA, MCVIDEO
Teltronic	MCPTT, MCDATA, MCVIDEO

Table 2. FRMCS MCX Clients Under Test

5.3 Evolved Multimedia Broadcast Multicast Services (eMBMS) Components

Organisation	Support
Athonet	

Table 3. Evolved Multimedia Broadcast Multicast Services (eMBMS) Components Under Test

5.4 Evolved Packet Core (EPC)

Organisation	Support
Athonet	MC-QCI, MC-APN

Table 4. Evolved Packet Core (EPC) Components Under Test

5.5 User Equipment (UE)

Organisation	Support
Leonardo	
Teltronic	MC-QCI, MC-APN, eMBMS

Table 5. Evolved Multimedia Broadcast Multicast Services (eMBMS) Components Under Test

5.6 Test Tools

Organisation	Support
Viavi Solutions	
Valid8	Network Simulator

Table 6. Testers Under Test

6 Test Infrastructure

6.1 Remote Test Infrastructure

The remote testing and pre-testing phase were enabled by the setup as shown in Figure 4:

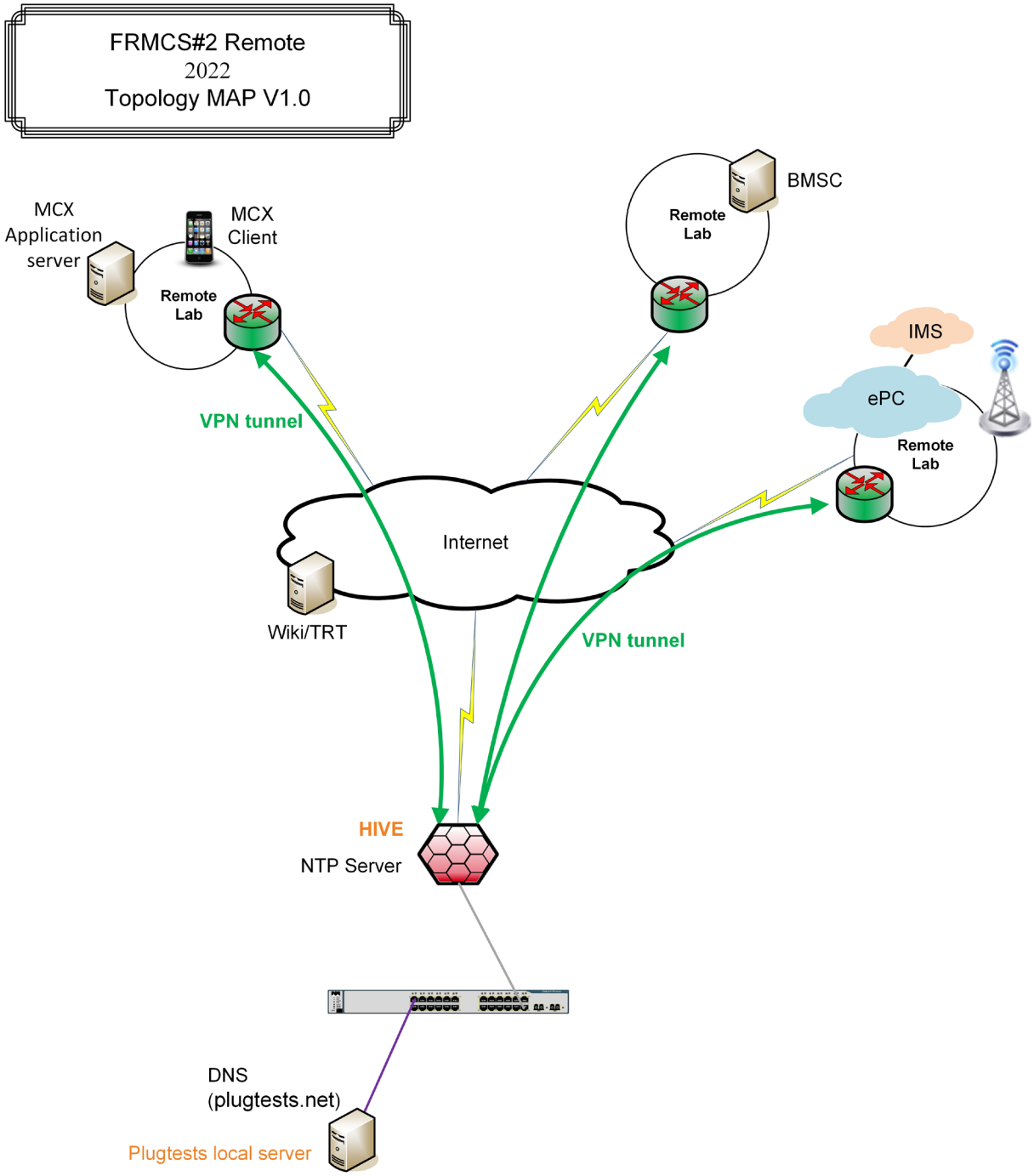


Figure 4. Remote Test Infrastructure

Once HIVE was deployed, a number of VPN tunnels were created to interconnect the equipment of the participants where the EUTs were running.

A total of 16 Remote Labs connected to the setup described above as a participant's lab.

7 Test Procedures

7.1 Remote Integration & Pre-testing Procedure

During the remote integration and pre-testing phase the following procedures were followed by the participating Equipment Under Test. Once the EUT documentation and HIVE connection had been successfully completed, the test cases from the test specifications were executed as part of the pre-testing

The progress of these procedures for the different combinations of EUTs was captured in the reporting function of TRT. The following Pre-Testing configurations were used in the pretesting phase

Config Name	Pre-testing Configuration
Config-FRMCS-OTT	FRMCS MCX Client + FRMCS MCX AS (SIP Core)

Table 7. Pre-testing Configuration

7.2 Interoperability Testing Procedure

During the Plugtests event, a daily Test Session Schedule was produced and shared via the TRT. Test Sessions were organised in several parallel tracks, ensuring that all participants had at least one Test Session scheduled any time. The different test configurations were used for the main event.

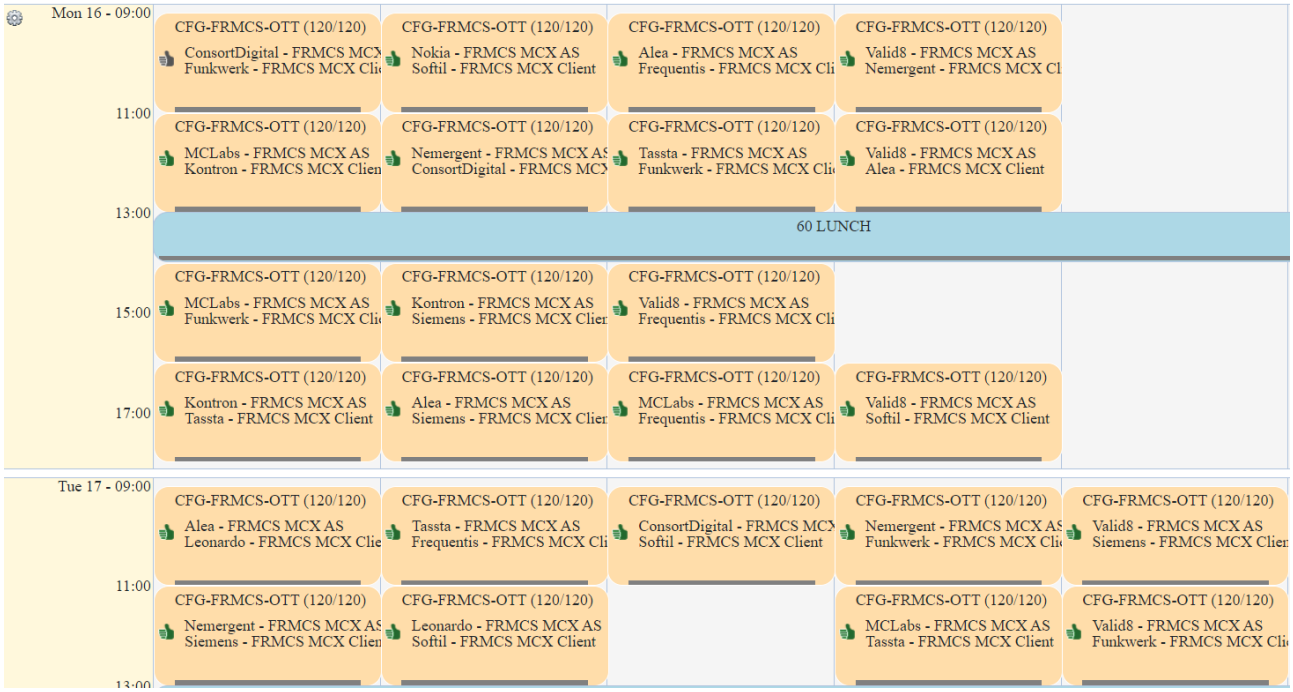


Figure 5. Daily Schedule & Test Sessions – example excerpt

Config Name	Main Test Configuration
Config-FRMCS-OTT	FRMCS MCX Client + FRMCS MCX AS (in-built SIP Core)
Config-FRMCS-WIFI	FRMCS MCX Client + FRMCS MCX AS (in-built SIP Core) + UE
Config- BMSC	BMSC + FRMCS MCX AS (in-built SIP Core)
Config-FRMCS-Scenarios	FRMCS MCX Client + FRMCS MCX AS (in-built SIP Core)
Config-Tester	Tester + FRMCS MCX Client

Table 8. Main Test Configurations

During each test session, for each tested combinations the Interoperability testing procedure was as follows:

1. The participating vendors opened the Test Session Report and the Test Plan.

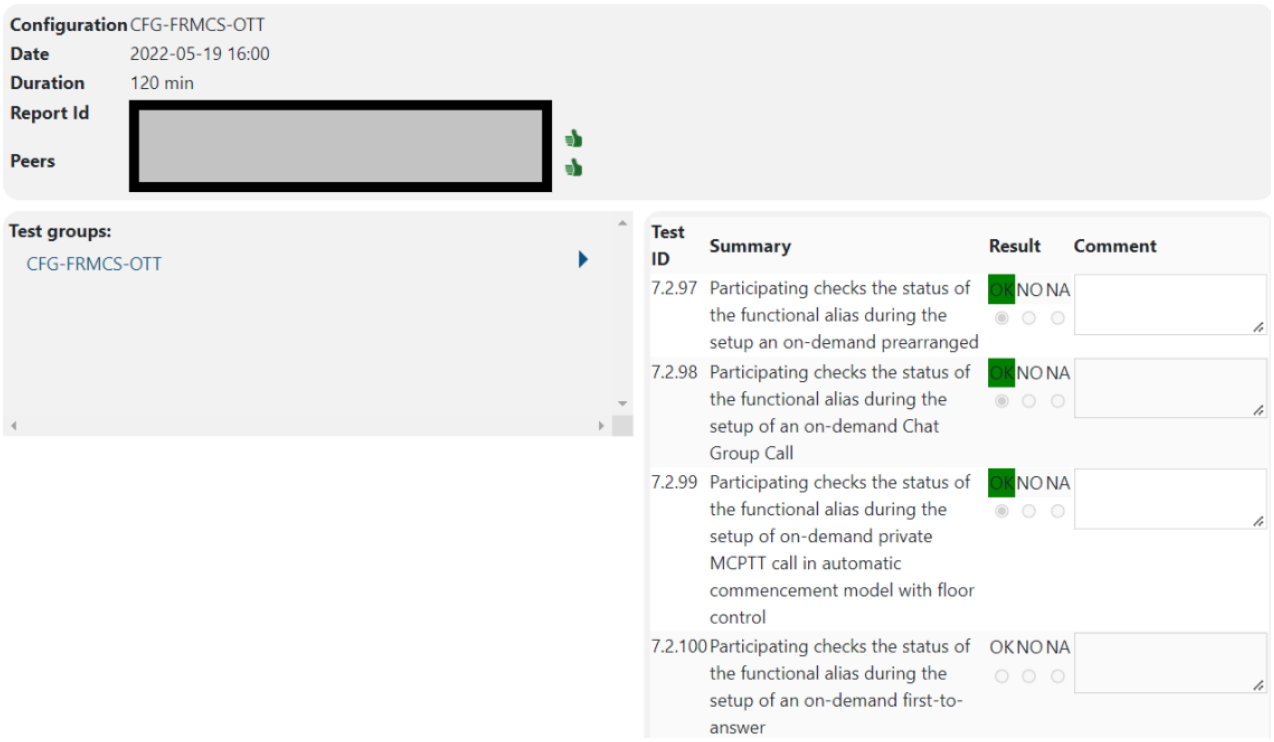


Figure 6. Test Session Report

2. For each Test in the Test Plan:

    a. The corresponding Test Description and EUT Configuration were followed.

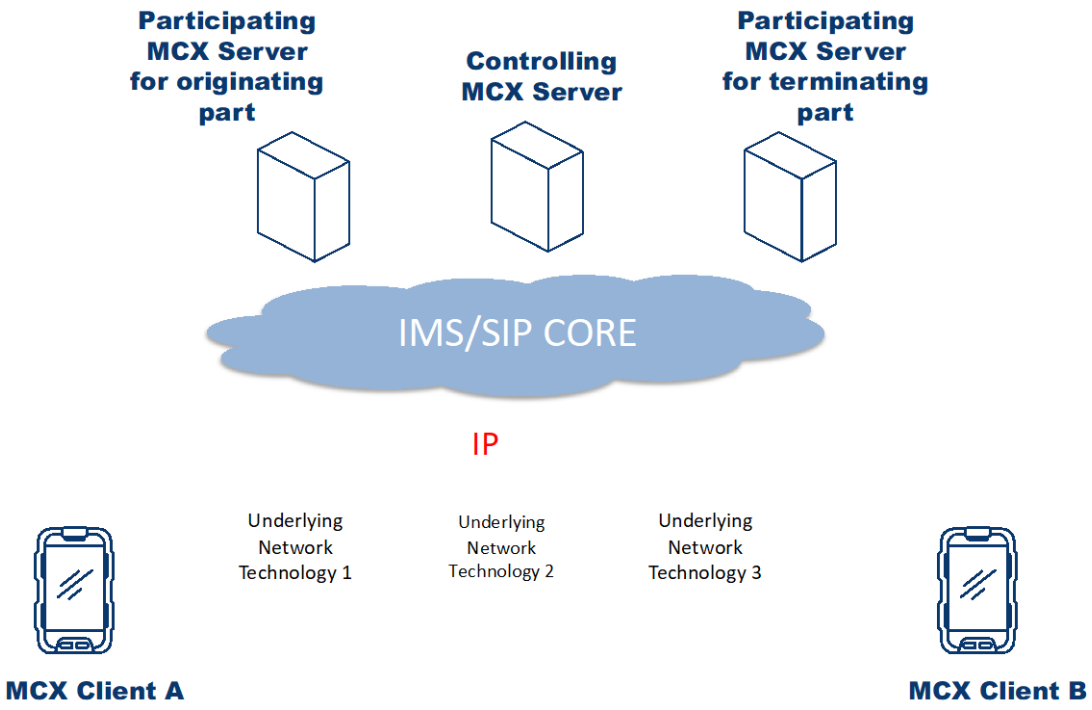


Figure 7. System Under Test (SUT) Configuration

Interoperability Test Description			
Identifier	REGRPREC/USERREG/01		
Test Objective	Verify IP connectivity, SIP core/IMS configuration and proper routing, SIP signalling for the user regroup request operation		
Configuration(s)	• CFG_ONN_OTT-1 (clause 5.2) • CFG_ONN_UNI-MC-LTE-1 (clause 5.3) • CFG_ONN_MULTI-MC-LTE-1 (clause 5.4)		
References	• SIP (see ETSI TS 124 229 [6] and other references in ETSI TS 124 379 [9]) • MCPT (see ETSI TS 124 380 [10] and other references in ETSI TS 124 379 [9]) • RTP (see ETSI TS 124 229 [6] and other references in ETSI TS 124 379 [9])		
Applicability	• MCPTT-Client_ONN-MCPTT-CALL, MCPTT-Client_AMR-WB • MCPTT-Client_AFFIL, MCPTT-Client_MCPTT-FC (clause 6.2) • MCPTT-Part_ONN-MCPTT-CALL, MCPTT-Part_AFFIL • MCPTT-Part_MCPTT-FC, MCPTT-Part_RX (CFG_ONN_UNI-MCLTE-1 only) • MCPTT-Part_GCSE (CFG_ONN_MULTI-MC-LTE-1 only) (clause 6.5) • MCPTT-Ctrl_ONN-MCPTT-CALL, MCPTT-Ctrl_AFFIL (clause 6.6)		
Pre-test conditions	• IP connectivity among all elements of the specific scenario • Proper configuration of the SIP core/IMS to forward the signalling to the specific controlling and participating servers • UEs properly registered to the SIP core/IMS and MCPTT system		
Test Sequence	**Step**	**Type**	**Description**
	1	stimulus	User 1 (mcptt_id_clientA@example.com) request the creation of a temporary group using the user regrouping with preconfigure group mechanism (4 users: A, B, C, D)
	2	check	SIP MESSAGE received at the MCPTT participating server of mcptt_id_clientA@example.com
	3	check	SIP MESSAGE received at the MCPTT controlling server
	4	check	The MCPTT controlling server creates separate lists grouped per terminating participating server and generates outgoing SIP MESSAGES to every participating
	5	check	Upon receiving the SIP MESSAGE very participating sends a SIP MESSAGE to the public identity of each of the users he is responsible for with no elements in the <users-for-regroup>
	6	check	Upon 200 OK the participatings the controlling considers the group is created with those users considered as affiliated
	7	verify	Temporary group built with user regrouping using a preconfigured group active

Figure 8. Test Description example

3. FRMCS equipment providers jointly executed the different steps specified in the test description and evaluated interoperability through the different IOP Checks prescribed in the Test Description

   b. The FRMCS equipment provider recorded the Test Result in the Test Session Report, as follows:

      i. OK: all IOP Checks were successful

      ii. NO: at least one IOP Check failed. A comment was requested.

      iii. NA: the feature was not supported by at least 1 of the involved EUTs. A comment was requested.

4. Once all the tests in the Test Session Report were executed and results recorded, the participants reviewed the Report and approved it.

8 Test Plan Overview

8.1 Introduction

This 2nd FRMCS Plugtests Test Plan was developed following ETSI guidelines for interoperability. Test cases were included comprising functional aliases, Multi-talker, MCData IP Connectivity, User Regrouping, MCData Message Store in different configurations.

The Test Plan was reviewed and discussed with participants during the preparation and pre-testing phase. Considering the huge number of resulting test cases and difference expected maturity of the implementations and differences from participants in the previous Plugtests event and new companies, vendors selected the subset of test cases to evaluate in a per-testing slot basis.

The following sections summarise the methodology used for identifying the different configuration and test objectives leading to different test cases subgroups.

8.2 Test configurations

The overall FRMCS ecosystem comprises both controlling and participating MCPTT/MCData/MCVideo application server(s), MCPTT/MCData/MCVideo Clients deployed over a generic SIP Core. Furthermore, a series of support servers were integrated in the so-called Common Services Core provide configuration, identity, group and key management capabilities. Note, again 3GPP Release-17 compliant On-Network operations only were considered.

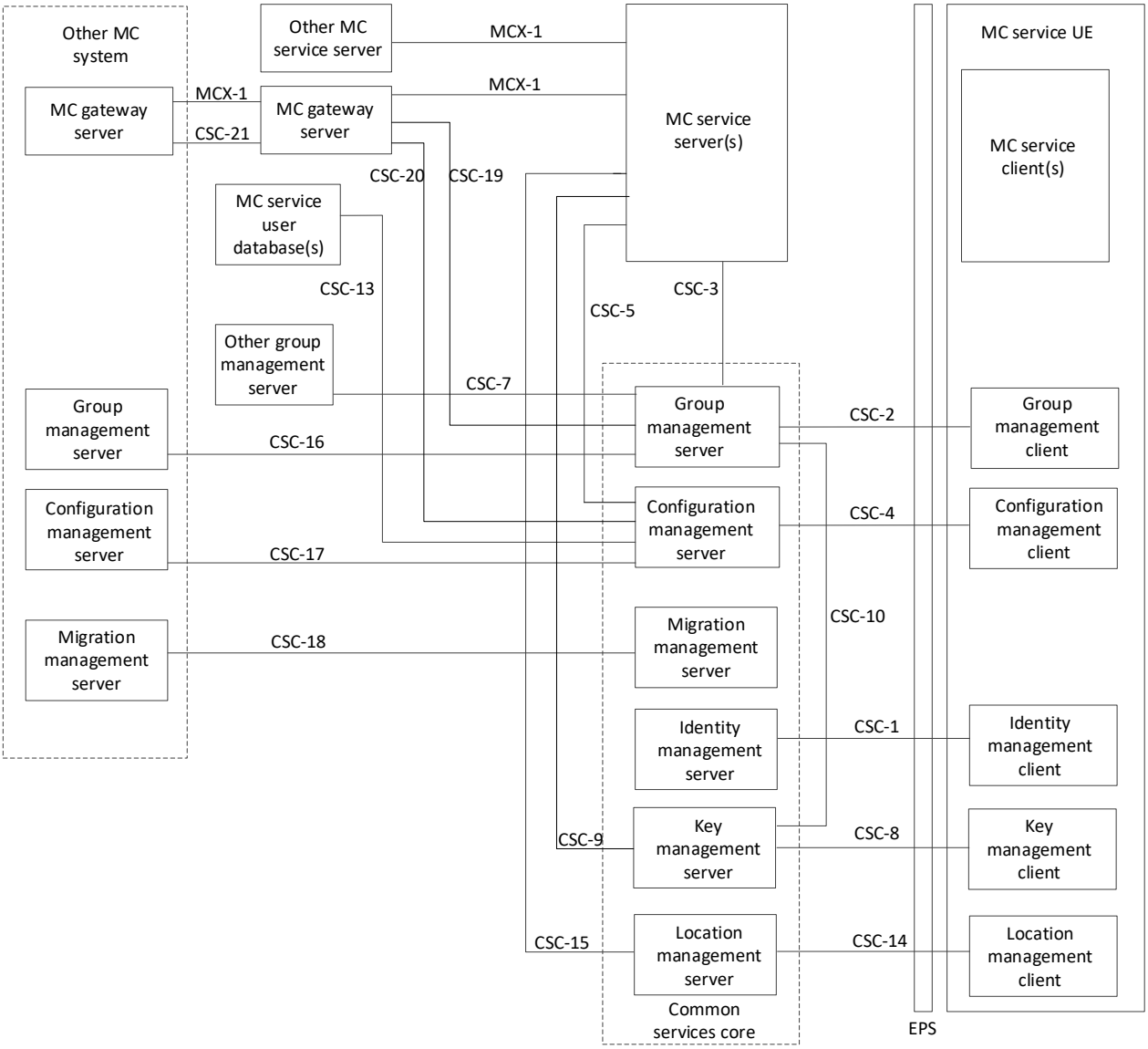


Figure 9. Functional model for application plane Figure 7.3.1-1 in 3GPP TS 23.280 [3].

Figure 7.3.1-1 in 3GPP TS 23.280 [3] describes the overall architecture and the reference points considered for the interoperability testing for any (MCPTT/MCData/MCVideo) Mission Critical Services (MCS). As can be seen, the resulting number of functional elements, interfaces and protocols involved is quite large. In order to focus on MCS signalling the following configuration were initially considered: MCPTT/MCData/MCVideo as an application service over IP networks (Over-the-Top).

8.2.1 Over-The-Top Configuration for On-Network calls (CFG_ONN_OTT-1)

This configuration considered On-Network Calls (ONN) with a pure Over-The-Top (OTT) approach. It emulated a scenario where any underlying network (i.e. commercial LTE, WiFi or any wired technology such as Ethernet) would provide a bit-pipe type only access. No QoS/prioritization enforcement neither access-layer multi/broadcasting capabilities would be provided (i.e. nor unicast PCC support or multicast mechanisms in LTE). Therefore, although not usable in a real world Mission Critical environment, it was used for connectivity tests since it did not require any binding between the IMS/SIP Core and the underlying LTE infrastructure and allowed both signalling and media plane parallel testing easily.

8.2.2 Unicast Mission Critical LTE for On-Network calls (CFG_ONN_UNI-MC-LTE-1)

In this configuration the LTE network (both EPC and eUTRAN) provided PCC capabilities and therefore enforced QoS policies in terms of prioritization and pre-emptiveness of Mission Critical unicast bearers. That included new Public Safety QCI 65/69 support in UEs and EPC/EUTRAN, and the availability of a PCRF with MCPTT compliant Rx/MCPTT-5 interface. Specific Rx/MCPTT-5 reference points and unicast bearer setup and update triggering mechanisms were tested using this configuration. Note that, although MCPTT only is mentioned and depicted in the following figure 10, MCVideo/MCData could follow the same approach.

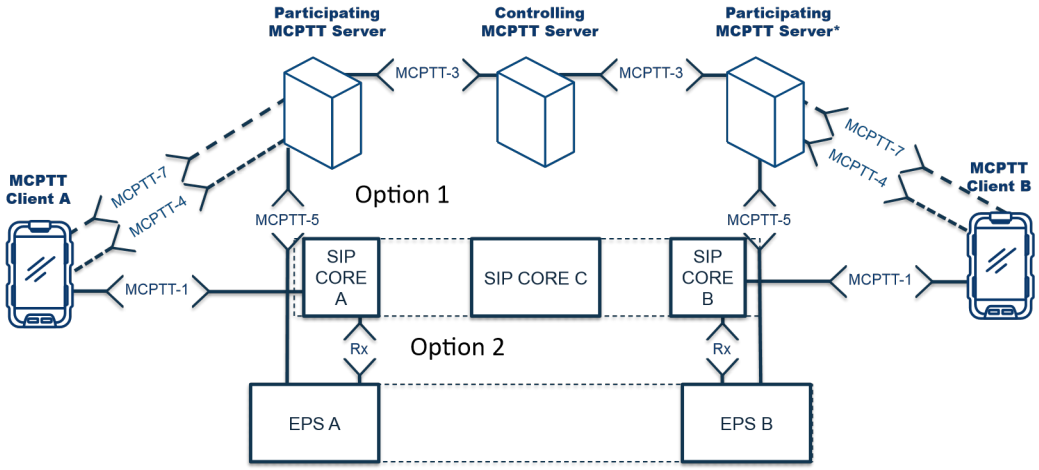


Figure 10. CFG_ONN_UNI-MC-LTE-1 configuration, MCPTT example

8.2.3 Multicast Mission Critical LTE for On-Network calls (CFG_ONN_MULTI-MC-LTE-1)

In this configuration LTE provided multicast capability including Rel. 14 (and beyond) LTE-A Pro eMBMS and needed interfaces both in the core side (MB2-C and MB2-U with the BM-SC) and in the eUTRAN/UE side. It was used to test eMBMS bearer setup and update related test cases.

NOTE: In this remote 2nd FRMCS Plugtests the unicast and multicast scenarios were limited to internal deployment due to the remote nature, so that they were not considered as different in the TRT tool.

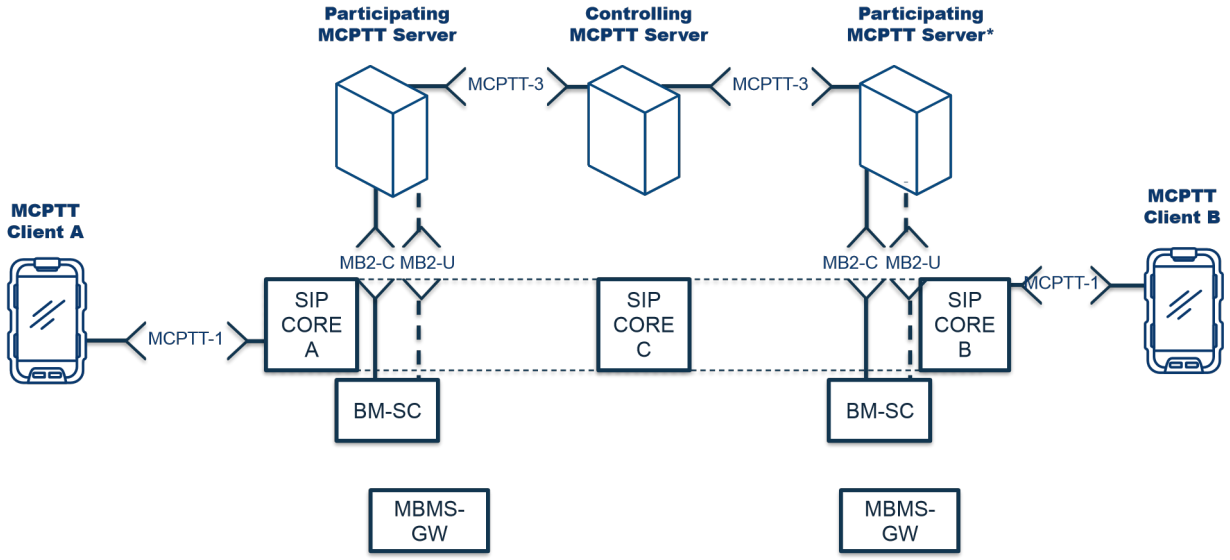


Figure 11. CFG_ONN_MULTI-MC-LTE-1 configuration, MCPTT example

Due to specific low level technical constraints (i.e. the availability of joint/split participating and controlling AS, usage of MCPTT-5 interface instead of Rx for the PCC or eMBMS support in the UE) the original configurations led to the ones described in Figure 11 according to the following mapping.

In order to deal with the different test setting according to the three aforementioned configurations and cover specific more complex test configuration involving different clients and Observer test cases, the following configuration modes were defined in the TRT tool.

Configuration	Resulting configuration mode in the Plugtests (TRT)
ONN-OTT	Config-FRMCS-OTT Config-BMSC Config-FRMCS-Scenarios Config-FRMCS-WIFI Config-Tester

Table 9. Mapping of scenario architecture configurations and Plugtests event practical configurations

8.2.5 Mapping of Test Cases to Test Case Numbers

The following tables collect the test cases from ETSI TS 103 564 [1] and the new developed test cases from the FRMCS Plugtests, grouped by test objective following the structure of the test specification document itself.

Please note that not all test cases from ETSI TS 103 564 [1] were in scope of the FRMCS Plugtests due to the focus of the event on rail-oriented features in OTT configuration. The results from the Observer Scenarios were not captures in the TRT.

Number	Name
Connectivity (CONN)	
7.2.97	Participating checks the status of the functional alias during the setup an on-demand prearranged MCPTT Group Call [CONN-MCPTT/ONN/GROUP/PREA/ONDEM/NFC/10]
7.2.98	Participating checks the status of the functional alias during the setup of an on-demand Chat Group Call [CONN-MCPTT/ONN/GROUP/CHAT/ONDEM/NFC/06]
7.2.99	Participating checks the status of the functional alias during the setup of on-demand private MCPTT call in automatic commencement model with floor control [CONNMCPTT/ONN/PRIV/AUTO/ONDEM/WFC/NFC/03]
7.2.100	Participating checks the status of the functional alias during the setup of an on-demand first-to-answer MCPTT call with floor control [CONN-MCPTT/ONN/FIRST/MANUAL/ONDEM/WFC/NFC/02]
7.2.101	MCPTT User includes the FA in an on-demand first-to-answer MCPTT call with floor control using pre-established sessions [CONN-MCPTT/ONN/FIRST/MANUAL/PRE/WFC/NFC/02]
7.2.102	MCPTT User includes the FA in an on-demand private MCPTT call in automatic commencement model with floor control [CONN-MCPTT/ONN/PRIV/AUTO/ONDEM/WFC/NFC/04]
7.2.103	MCPTT User calls a FA using an on-demand first-to-answer MCPTT call with floor control [CONN-MCPTT/ONN/FIRST/MANUAL/ONDEM/WFC/NFC/03]
7.2.104	MCPTT User calls a FA using an on-demand first-to-answer MCPTT call without floor control [CONN-MCPTT/ONN/FIRST/MANUAL/ONDEM/WOFC/02]
7.2.105	MCPTT User calls a FA using an on-demand first-to-answer MCPTT call with floor control using pre-established sessions [CONN-MCPTT/ONN/FIRST/MANUAL/PRE/WFC/NFC/03]
7.2.106	MCPTT User calls a FA using a pre-established first-to-answer MCPTT call in manual commencement mode without floor control [CONN-MCPTT/ONN/FIRST/MANUAL/PRE/WOFC/02]
7.2.107	A not-authorized MCPTT User initiates an on-demand private MCPTT call in automatic commencement model with floor control [CONN-MCPTT/ONN/PRIV/AUTO/ONDEM/WFC/NFC/05]
7.2.108	A not-authorized MCPTT User initiates an on-demand private MCPTT call in manual commencement mode with floor control [CONN-MCPTT/ONN/PRIV/MANUAL/ONDEM/WFC/NFC/02]
7.2.109	A not-authorized MCPTT User initiates a pre-established private MCPTT call in automatic commencement mode with floor control [CONN-MCPTT/ONN/PRIV/AUTO/PRE/WFC/NFC/02]
7.2.110	A not-authorized MCPTT User initiates a pre-established private MCPTT call in manual commencement mode with floor control [CONN-MCPTT/ONN/PRIV/MANUAL/PRE/WFC/NFC/02]
7.2.111	A not-authorized MCPTT User initiates an on-demand private MCPTT call in automatic commencement mode without floor control [CONN-MCPTT/ONN/PRIV/AUTO/ONDEM/WOFC/02]
7.2.112	A not-authorized MCPTT User initiates an on-demand private MCPTT call in manual commencement mode without floor control [CONN-MCPTT/ONN/PRIV/MANUAL/ONDEM/WOFC/02]
7.2.113	A not-authorized MCPTT User initiates a pre-established private MCPTT call in automatic commencement mode without floor control [CONN-MCPTT/ONN/PRIV/AUTO/PRE/WOFC/02]
7.2.114	A not-authorized MCPTT User initiates a pre-established private MCPTT call in manual commencement mode without floor control [CONN-MCPTT/ONN/PRIV/MANUAL/PRE/WOFC/02]
7.2.115	A not-authorized MCPTT User initiates an on-demand private MCPTT emergency call in automatic commencement model with floor control [CONN-MCPTT/ONN/PRIV/AUTO/ONDEM/WFC/NFC/06]
7.2.116	Handling of non-acknowledged user information during an on-demand prearranged MCPTT Group Call [CONN-MCPTT/ONN/GROUP/PREA/ONDEM/NFC/11]

Number	Name
7.2.117	Handling of TNG1 timer during the setup of an on-demand prearranged MCPTT Group Call [CONN-MCPTT/ONN/GROUP/PREA/ONDEM/NFC/12]
7.2.118	Handling of non-acknowledged user information during a prearranged MCPTT Group Call using preestablished session [CONN-MCPTT/ONN/GROUP/PREA/PRE/NFC/05]
7.2.119	Handling of TNG1 timer during the setup of a prearranged MCPTT Group Call using pre-established session [CONN-MCPTT/ONN/GROUP/PREA/PRE/NFC/06]
7.2.120	MCData client establishes a IP Connectivity session with another MCData client [CONNMCDATA/ONN/IPCONN/01]
7.2.121	MCData client establishes a IP Connectivity session with another MCData client by using the target IP Information [CONN-MCDATA/ONN/IPCONN/02]
7.2.125	MCPTT user to send a remotely initiated private call request to the remote MCPTT user [CONN-MCVIDEO/ONN/REMOTE/PRIV/01]
7.2.126	MCPTT user requests to transfer an ongoing MCPTT private call to a target MCPTT user [CONN-MCVIDEO/ONN/TRANSF/PRIV/01]
7.2.127	MCPTT user decides to forward an incoming MCPTT private call to a new target MCPTT ID [CONN-MCVIDEO/ONN/FORW/PRIV/01]
Floor Controlling (FC)	
7.3.6	Sharing/Display of FA during basic FC operations [FC/FA/BASIC/01]
Multi-Talker (MT)	
7.3.7	Multi-talker basic operation [FC/MT/BASIC/01]
Sharing Location Information (LOC)	
7.3.8	Sharing location information during FC operations [FC/LOC/BASIC/01]
7.3.9	Sharing location information during multi-talker FC operations [FC/MT/LOC/BASIC/01]
Registration and Authorization (RegAuth)	
7.4.4	MCPTT service server limits the number of simultaneous successful service authorisations while using third-party registration [REGAUTH/3PRTYREG/REGISTER/02]
7.4.5	MCPTT service server limits the number of simultaneous successful service authorisations while using PUBLISH mechanism [REGAUTH/PUBLISH/REGISTER/02]
Affiliation (AFFIL)	
7.7.6	Affiliation change triggered by a functional-alias activation criteria [AFFIL/CHANGE/04]
7.7.7	Affiliation change triggered by a functional-alias deactivation criteria [AFFIL/CHANGE/05]
Functional Aliases (FA)	
7.13.1	MCPTT user requests to activate one or more functional aliases [FA/CHANGE/01]
7.13.2	MCPTT user requests to deactivate one or more functional aliases [FA/CHANGE/02]
7.13.3	MCPTT user refreshes the interest on one or more functional aliases [FA/CHANGE/03]
7.13.4	MCPTT user takes over a functional alias [FA/CHANGE/04]
7.13.5	MCPTT user requests to activate one or more functional aliases upon entering a location area [FA/LOCCHANGE/01]
7.13.6	MCPTT user requests to deactivate one or more functional aliases upon entering a location area [FA/LOCCHANGE/02]
7.13.7	MCPTT user determines the functional aliases successfully activated [FA/DET/01]
7.13.8	MCPTT user determines the functional aliases successfully activated for another user [FA/DET/02]
7.13.9	MCPTT server requests a resolution of the Functional alias from the MCPTT server owning that FA [FA/RESOL/01]
7.13.10	Automatic deactivation of FA [FA/CHANGE/05]
MCData Message Store (MCDATAMS)	
7.16.18	Message notification client in the MCData Client creates a notification channel [MCDATAMS/NOTCH/01]
7.16.19	Message notification client in the MCData Client deletes a notification channel [MCDATAMS/NOTCH/02]
7.16.20	Message notification client in the MCData Client updates a notification channel [MCDATAMS/NOTCH/03]
7.16.21	Message notification client in the MCData Client opens a notification channel [MCDATAMS/NOTCH/04]
7.16.22	MCData message store function sends a notification of changes using notification channel [MCDATAMS/SYNC/03]
FRMCS scenarios	
10.1	Initiation by a mobile user of a railways emergency communication, client driven, alert and call [FRMCS/REC/CLIENT/01]
10.2	Initiation by a mobile user of a railways emergency communication, client driven, combined alert and call [FRMCS/REC/CLIENT/02]
10.3	Initiation by a mobile user of a railways emergency communication, server driven, alert and call [FRMCS/REC/SERVER/01]

Number	Name
10.4	Initiation by a mobile user of a railway's emergency communication, server driven, combined alert and call [FRMCS/REC/SERVER/02]

Table 10. Mapping of Test Case Numbers to Test Case Names

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 60 Test Sessions were run: that is, 60 different combinations based on different configurations in Test Scope: FRMCS MCX Client, FRMCS MCX Application Server (Participating and Controlling), and SIP Core were tested for interoperability. Overall, 338 test executions were conducted and reported interoperability results.

The table 11 below provides the overall results (aggregated data) from all the Test Cases run during all the Test Sessions with all the different combinations of Equipment Under Test from all the participating companies.

Among the executed Test Cases, the possible results were “OK”, when interoperability was successfully achieved and “NO” (Not OK) when it was not.

Interoperability		Totals
OK	**NO**	**Run**
320 (94.7%)	18 (5.3%)	338

Table 11. Overall Results

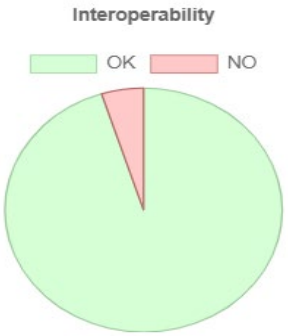


Figure 12. Overall results (%)

A overall interoperability success rate of 94.7% was achieved, which indicates a very high degree of compatibility among the participating implementations (EUTs) in the areas of the Test Plan where features were widely supported and the test cases could be executed in most of the Test Sessions. In the next clauses, we will see that this high rate is also a consequence of the good preparation and involvement of participants during the remote integration and pre-testing phase of the Plugtests.

9.2 Results per Test Configuration

The table 12 below provides the results for each test configuration in the scope of the Plugtests event. The below configurations are defined in clause 7.2.

	Interoperability		
	OK	NO	Run
CFG-FRMCS-OTT	311 (94.8%)	17 (5.2%)	328
CFG-FRMCS-WIFI	9 (100.0%)	0 (0.0%)	9
CFG-Tester	0(0.0%)	0 (0.0%)	0
CFG-FRMCS-Scenarios	0(0.0%)	1 (100.0%)	1

Table 12. Results per Test Configuration

The table shows that very high execution and interoperability rates for different Test Configurations were achieved.

Note: Results from the tester stream were not reported in the TRT.

9.3 Results per Test Case

The table 13 below provides the results for each test case in the scope of the Plugtests event. Test Cases numbering is referred from ETSI TS 103 564.

	Interoperability		Totals
	OK	NO	Run
7.2.97	14 (100.0%)	0 (0.0%)	14 (73.7%)
7.2.98	1 (33.3%)	2 (66.7%)	3 (27.3%)
7.2.99	12 (100.0%)	0 (0.0%)	12 (63.2%)
7.2.100	3 (75.0%)	1 (25.0%)	4 (40.0%)
7.2.101	1 (100.0%)	0 (0.0%)	1 (11.1%)
7.2.102	15 (93.8%)	1 (6.3%)	16 (69.6%)
7.2.103	11 (100.0%)	0 (0.0%)	11 (57.9%)
7.2.104	16 (94.1%)	1 (5.9%)	17 (77.3%)
7.2.105	1 (100.0%)	0 (0.0%)	1 (12.5%)
7.2.106	1 (50.0%)	1 (50.0%)	2 (25.0%)
7.2.107	6 (100.0%)	0 (0.0%)	6 (54.5%)
7.2.108	6 (100.0%)	0 (0.0%)	6 (60.0%)
7.2.109	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.2.110	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.2.111	3 (100.0%)	0 (0.0%)	3 (27.3%)
7.2.112	2 (100.0%)	0 (0.0%)	2 (20.0%)
7.2.113	3 (100.0%)	0 (0.0%)	3 (37.5%)
7.2.114	2 (100.0%)	0 (0.0%)	2 (25.0%)
7.2.115	4 (100.0%)	0 (0.0%)	4 (40.0%)
7.2.116	3 (100.0%)	0 (0.0%)	3 (37.5%)
7.2.117	4 (100.0%)	0 (0.0%)	4 (44.4%)
7.2.118	3 (100.0%)	0 (0.0%)	3 (37.5%)
7.2.119	3 (100.0%)	0 (0.0%)	3 (37.5%)
7.2.120	2 (100.0%)	0 (0.0%)	2 (20.0%)
7.2.121	2 (100.0%)	0 (0.0%)	2 (20.0%)
7.2.125	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.2.126	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.2.127	0 (0.0%)	0 (0.0%)	0 (0.0%)

7.3.6	14 (93.3%)	1 (6.7%)	15 (88.2%)
7.3.7	3 (60.0%)	2 (40.0%)	5 (38.5%)
7.3.8	3 (100.0%)	0 (0.0%)	3 (27.3%)
7.3.9	2 (100.0%)	0 (0.0%)	2 (20.0%)
7.4.4	3 (100.0%)	0 (0.0%)	3 (37.5%)
7.4.5	2 (100.0%)	0 (0.0%)	2 (25.0%)
7.7.6	1 (100.0%)	0 (0.0%)	1 (12.5%)
7.7.7	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.13.1	44 (97.8%)	1 (2.2%)	45 (93.8%)
7.13.2	37 (94.9%)	2 (5.1%)	39 (90.7%)
7.13.3	16 (100.0%)	0 (0.0%)	16 (76.2%)
7.13.4	7 (100.0%)	0 (0.0%)	7 (53.8%)
7.13.5	2 (66.7%)	1 (33.3%)	3 (27.3%)
7.13.6	2 (100.0%)	0 (0.0%)	2 (20.0%)
7.13.7	40 (93.0%)	3 (7.0%)	43 (91.5%)
7.13.8	14 (100.0%)	0 (0.0%)	14 (58.3%)
7.13.9	1 (100.0%)	0 (0.0%)	1 (11.1%)
7.13.10	11 (91.7%)	1 (8.3%)	12 (66.7%)
7.16.18	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.16.19	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.16.20	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.16.21	0 (0.0%)	0 (0.0%)	0 (0.0%)
7.16.22	0 (0.0%)	0 (0.0%)	0 (0.0%)
10.1	0 (0.0%)	0 (0.0%)	0 (0.0%)
10.2	0 (0.0%)	1 (100.0%)	1 (100.0%)
10.3	0 (0.0%)	0 (0.0%)	0 (0.0%)
10.4	0 (0.0%)	0 (0.0%)	0 (0.0%)
TESTER	0 (0.0%)	0 (0.0%)	0 (0.0%)

Table 13. Results per Test Case

10 Plugtests Observations

As a result of the Plugtests event activities some issues in 3GPP Technical Specifications (TSs) and related standards were identified together with practical deployment problems that may demand some clarification or feedback from the related SDOs. We have classified those aspects into the following two categories:

- **Observations to MCX Standards**: Missing, erroneous or ambiguous definition of procedures in 3GPP's MCPTT TSs.
- **Technical constraints**: Related to implementation issues, not covered by the standards, but which need to be faced by vendors in most deployments.

The reader should note that 3GPP Release-17 TS approved by March 2022 were considered for the 2nd FRMCS Plugtests event.

The 2nd FRMCS Plugtests event team wants to thank all the participants in the Plugtests for kindly sharing the following lessons learned. Specific actions towards pushing this feedback to relevant TSGs in 3GPP have already been started at the time of the release of this report.

10.1 Standards issues

10.1.1 Remote private call response SIP MESSAGE allegedly sent by the target client to the participating responsible from original requesting client

According to clause 11.1.7.2.2 in 3GPP TS 24379 (17.6.0) last subclause 3) the remote client shall set the Request-URI to the public service identity identifying the participating MCPTT function serving the MCPTT user identified by the MCPTT ID contained in the <mcptt-calling-user-id> element in the application/vnd.3gpp.mcptt-info+xml MIME body of the received SIP MESSAGE request

That would mean the client (mcptt-client-B) is capable of directly routing the message back to the originating participating (mcptt-client-A).

Furthermore, in Section 11.1.7.4, it looks like the controlling should be responsible for handling the response.

10.1.2 Explicit mentioning of how mcptt-request-uri is fulfilled by controlling in private call forwarding

Clause 11.1.9.4 in 3GPP TS 24379 (17.6.0) does not mention how the <mcptt-request-uri> is populated (based on RLS) although later Request-URI is mentioned and also the terminating participating.

10.1.3 Clarification of the SIP exchange after the ringing when the call is forwarded

After the manual commencement derive 180 ringing the original call is not completed. The SIP behaviour should be clarified since the usual SIP forwarding mechanism (i.e. 302) is not used.

10.1.4 Channel type in OMA REST NOTIFICATION CHANNELS procedure

Clause 6.1.5 of OMA-TSREST_NetAPI_NotificationChannel-V1_0-20200319-C defines the mechanism to create a notification channel. Which ChannelType for MCData are not mentioned..

10.1.5 Track Option 3 in 10.3/10.4 and clarify the affiliation mechanism for the user triggering the initial alert to generic group name

In test case 10.3 the notification of entry into an emergency alert area following Section 6.3.2.4.1 in ETSI TS 124 379 [9] was intended to be used. However, for the FRMCS#2 Plugtests since <associated-group-id> is missing in 6.3.2.4.1, no implicit affiliation is added and C1-222074 marked as postponed in C1#134-e waiting for needed Stage 2 CRs

different tentative options are considered: OPTION 1: the original 6.3.2.4.2 mechanism (as in [FRMCS/REC/CLIENT/01] but triggered on emergency initiation time) will be used. OPTION 2: Following original 6.3.2.4.1 all users receiving notification of entry into an emergency alert area would initiate the emergency alert and carry out the alerted group selection heuristic as in [FRMCS/REC/CLIENT/01] but in the client side (and eventually following NOTE 4: Based on implementation the MCPTT client can subsequently automatically originate an MCPTT emergency group call as specified in clause 10.1.1.2). Once the proper alerted group is selected and (n) alert are initiated later in the participating (see Clause 12.1.2.1 Subclause 3)) if the MCPTT user is not affiliated with the MCPTT group as determined by clause 9.2.2.2.11, shall perform the actions specified in clause 9.2.2.2.12 for implicit affiliation. OPTION 3: Assume <associated-group-id> is included.

NOTE how the original client triggering the generic alert gets affiliated is FFS.

10.2 Technical Constraints

None identified during this Plugtests.

11 Observer Program

The Observers contributed to the FRMCS#2 Plugtests in the definition of the scope and scenarios, in the Observer Program and for the Observer demo.

11.1 Observer Presentations

Observer program is a presentation program during FRMCS and MCX Plugtests event which focused on the deployment plans and challenges of mission critical services. The observer program provided a platform to the various stake holders in the critical communication industry to discuss the progress of MCS technology.

During the FRMCS#2 Plugtests no observer presentations were done. Observer presentations are planned again for the next MCX Plugtests.

11.2 Observer Demo

The Observer Demo was a possibility for vendors to present their solutions and rail features to the observers. Interested vendors could book 40 minutes slots during the half day on 19 May 2022. Table 14 shows the observer demo overview.

Vendor #1	Vendor #2
LEONARDO	ALEA
ALEA	ATHONET

Table 14. Observer Demo

History

Document history		
V0.1.0	23/05/2022	First Draft
V0.2.0	31/05/2022	Stable Draft
V0.3.0	07/06/2022	Final Draft
V1.0.0	13/06/2022	Final report published