ETSI Plugtests Report V1.1.0 (2023-11)

8th ETSI MCX Plugtests
Malaga, Spain
09 October – 13 October 2023

ETSI

Keywords
Testing, Interoperability, Mission-Critical, LTE,
MCPTT, MCData, MCVideo, 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 capabilities of Mission Critical Push to Talk (MCPTT), Mission Critical Data (MCData) and Mission Critical Video (MCVideo) – together abbreviated as MCX services – were tested during the eighth MCX Plugtests from 09th October to 13th October 2023 at the University of Malaga (UMA) in Spain using 4G and 5G test networks. 1508 test cases were executed between vendors, based on 3GPP Release-17.

The 8th ETSI MCX Plugtests have concluded with a success rate of 95.0% of the executed tests in the validation of 3GPP mission critical services vendor interoperability. More than 180 delegates participated during the 8th MCX Plugtests event on-site in Malaga and off-site from their labs.

These tests are essential to ensure seamless access to mission critical services over 4G and 5G networks across different vendors' products and implementations.

The MCX ETSI Plugtests series is the first independent testing of public safety and other mission critical services over LTE and 5G networks. FRMCS (Future Rail Mobile Communications System) features, Interworking Function IWF to LMR systems like TETRA. Off-network (device to device communication), eMBMS (multicast) and Conformance test tools were particularly tested in these 8th MCX Plugtests. The preparations for the eighth Plugtests started in June 2023, were followed by two weeks of integration with the test network in September 2023, a one-week pre-testing in October 2023, and were finalized with a one week of face-to-face end-to-end interoperability testing with 4G and 5G test networks in Malaga. For the first time Off-network testing was performed during the MCX Plugtests and different eMBMS components were integrated into a multivendor test networks setup and tested end-to-end.

The tests were based on 3GPP Release-17, and 1508 tests were executed between the different vendors in more than 170 test sessions. The test cases have been amended with additional off-network test scenarios which will be included in a future version of ETSI TS 103 564 (after the ETSI committee TCCE approval). A total of more than 360 test cases are now available for the MCX and FRMCS Plugtests. Besides the MCPTT, MCData and MCVideo Application Servers and Clients, the testing also included devices, railways-oriented features, Interworking with TETRA, IMS (IP Multimedia Subsystem), eMBMS (Evolved Multimedia Broadcast Multicast Services) components, Server to Server, off-network and inter-MCX communication. Both 4G and 5G networks were used as transport mechanism. A test stream was dedicated for 3GPP RAN5 conformance testing.

Additionally, gathered observations from the Plugtests events provide essential feedback to 3GPP Working Groups as work continues in mission critical communication specifications.

The testing during the 8th MCX Plugtests was complemented by an observer program with presentations, round-table discussions and demos for the observers.

This eight MCX Plugtests was organized by ETSI with the support of the European Union, EFTA, TCCA, EUTC UIC.

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

The next FRMCS and MCX Plugtests events are planned for June and November 2024 respectively.

The companies participating in this MCX Plugtests registered the following equipment for the indicated Test Streams:

MCX Application Servers:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Airbus	X	X			n/a	

MCX Application Servers:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Alea	X	X		X	n/a	
Aselsan	X				n/a	
Consort Digital	X				n/a	
Cybertel Bridge	X				n/a	
Frequentis	X				n/a	
HMF	X				n/a	X
Hytera	X	X	X		n/a	
Kontron	X	X	X		n/a	
MCLabs	X	X			n/a	X
Motorola	X	X		X	n/a	X
Nemergent	X	X		X	n/a	X
Samsung	X				n/a	
Streamwide	X	X		X	n/a	X
TASSTA	X	X			n/a	
Valid8	X	X	X		n/a	

MCX Application Clients:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Alea	X	X			X	X
Alstom						X
Consort Digital	X					
Eviden	X		X	X		
Hytera	X	X	X			
Kontron	X	X	X			
MCLabs	X				X	X
Nemergent	X	X		X	X	X
Sepura	X					
Softil	X				X	
TASSTA	X	X				
Valid8	X				X	

User Equipment (UE):	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Device:						
Aselsan	X					
Crosscall	X	X	X			X
Funkwerk	X	X	X			
Hytera	X	X	X			
Qualcomm					X	
Sepura	X					
Cab Radio:						
Consort Digital	X			n/a		
Teltronic	X		X	n/a		X
On-Board Gateway:						
Alstom	n/a	n/a	X	n/a	n/a	X

Land Mobile Radio (LMR):	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Rohill (TETRA)	n/a	n/a	n/a	X	n/a	X
Eviden (Simulator)	n/a	n/a	n/a	X	n/a	

Evolved Node B (eNB):	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Enensys	X	n/a	n/a		n/a	n/a
Teltronic	X	n/a	n/a		n/a	n/a
Test System (UMA)	X	n/a	n/a		n/a	n/a

Next Generation Node B (gNB):	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Test System (UMA)	n/a	X	X		n/a	n/a

Evolved Packet Core (EPC):	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Teltronic	X	n/a	n/a		n/a	n/a
Test System (UMA)	X	n/a	n/a		n/a	n/a

5G Core:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Athonet	n/a	X	X		n/a	n/a

Evolved Multimedia Broadcast Multicast Services (eMBMS) Components:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Aselsan	X	n/a	n/a		n/a	n/a
Enensys	X	n/a	n/a		n/a	n/a
Teltronic	X	n/a	n/a		n/a	n/a

Dispatcher:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
Alstom (TS-GW)			X		n/a	
Consort	X				n/a	
Eurofunk	X				n/a	
Eviden	X				n/a	
Frequentis	X	X	X		n/a	X
Kolibri	X	X			n/a	X
Kontron		X	X		n/a	
Softil	X		X		n/a	
Tassta	X	X			n/a	
Teltronic	X	X	X		n/a	X
Zetron	X				n/a	

Test Tool Vendors:	**Stream A** MCX over 4G	**Stream B** MCX over 5G	**Stream C** FRMCS/5G	**Stream D** IWF	**Stream E** Off-network	**Stream F** Test Tools
MCS-TaaSting	n/a	n/a	n/a	n/a	n/a	X
Valid8	n/a	n/a	n/a	n/a	n/a	X

The following observer organsiations participated in this Plugtests:

- A.S.T.R.I.D, Public saftey network operator, Belgium
- ADIF, Administrador de Infraestructuras Ferroviarias, Spain
- AstaZero – RISE Research Institutes of Sweden, Sweden
- BANE NOR SF, Railway Infrastructure Company, Norway
- BDBOS, Federal Agency for Public Safety Digital Radio, Germany
- Cybersecurity and Infractructure Security Agency / Department of Homeland Security, USA
- Directorate for Civil Protection (DSB), Norway
- Direzione Centrale Anticrimine della Polizia di Stato, Central Anti-Crime Directorate of the State Police, Italy
- Erillisverkot, Public saftey network operator, Finland
- GCF, Global Certification Forum
- Home Office, United Kingdom
- INECO, Spain
- French Ministry of Interior, France
- MSB, Swedish Civil Contingencies Agency, Sweden
- National Police ICT-unit, Norway
- Direzione Centrale Anticrimine della Polizia di Stato, Italy
- SNCF Reseau, Railway operator research, France
- State Infocommunication Foundation, Public saftey network operator, Estonia
- TCCA, The Critical Communication Association
- Trafikverket, Swedish Transport Administration, Sweden


Observers
ERILLISVERKOT
dsb
Norwegian Directorate for Civil Protection
ETSI
astrid
AstaZero
MSB
Swedish Civil Contingencies Agency
SNCF RÉSEAU
BANE NOR
TCCA
POLICE NATIONALE
RIKS
MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité
Home Office
adif
Federal Agency for Public Safety Digital Radio
smit
Nasjonal kommunikasjons-myndighet
ineco
GCF
Test Certify Connect
TRAFIKVERKET
©ETSI 2023 – All rights reserved

1. Introduction

Mission Critical Push To Talk (MCPTT) is a 3GPP standardized voice service for mobile radio systems which ensures that LTE (and 5G) systems support mission-critical communications.

The Global Mission-Critical Communication Market was valued at USD 17.03 Billion in 2022 and is estimated to reach USD 27.87 Billion by 2028 growing at a CAGR of 8.6% during the forecast period 2022–2028, 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 standardized by 3GPP in Release-13. Mission Critical Video and Mission Critical Data were standardized in Release-14. With the standardization of MCS (Mission-Critical PTT, Video & Data), IOPS (Isolated Operation for Public Safety), and other critical communications features by 3GPP, LTE and 5G NR networks are increasingly gaining recognition as an all-inclusive communications platform for public safety, rail, utilities and other critical communications sectors.

Preparations for the 8th ETSI MCX Plugtests event started in June 2023 with the registrations of vendors and observers. During bi-weekly conference calls from June to October 2023 the setup of the tests, the test specification and organizational issues were agreed between the participants. Before the main event, the vendors have done integration with test network and 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 8th MCX 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 8th MCX Plugtests event wiki: https://wiki.plugtests.net/8th-MCX-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:

- MCX Application Servers (MCX AS)
- MCX Clients
- Evolved Node B (eNB)
- Next Generation Node B (gNB)
- User Equipment (UE) – including sidelink functionality
- Land Mobile Radio (LMR) Systems – TETRA
- Evolved Packet Core (EPC)
- 5G Core (5GC)
- IP Multimedia Subsystem (IMS)
- Broadcast Multicast Service Center (BMSC)
- Evolved Multicast/Broadcast Multimedia Service Gateway (eMBMS-GW)
- MCX Conformance Test Tools
- Dispatchers
- CabRadios
- OB-GW (On-Board Gateway)

- TS-GW (Trackside Gateway)

In this Plugtests the railways-oriented Application Servers and Clients were evaluated in a dedicated Rail test stream (Stream C) and Interworking with LMR systems was evaluated in another dedicated IWF test stream (Stream D).

Note: TETRA IWF implementations were based on draft standards from ETSI TCCA.

Stream A and B was available for vendors to evaluate their equipment for end-to-end interoperability testing over 4G and 5G networks respectively.

For the first time off-network functionality (device to device communication over the PC5 sidelink) was tested in a dedicated off network test stream (Stream E), which was available for sidelink UEs and MCX off network client vendors to test off network testing.

A dedicated Test Tools test stream (Stream F) was available for test tool vendors and MCX server and client vendors to check their tools and the conformance of their implementations with these test tools.

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 8th MCX Plugtests 8 additional test cases were developed by ETSI for Off networking testing. In total, the MCX test specification has now 367 test cases. See clause 8. An updated version of the test specification will be published as a new version of ETSI document ETSI TS 103 564 (after ETSI TC TCCE approval).

1508 tests were conducted by the vendors. 95.0% 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 are very valuable because they give the vendors valuable information to improve their implementations. They also help to discover errors or ambiguities in the standards and to clarify and improve the specifications.

ETSI plan to conduct more FRMCS/MCX Plugtests in the future. The next FRMCS/MCX Plugtests sessions are planned for Q2 and Q4 2024. Vendors and observers who have not participated in the previous MCX Plugtests events are welcomed and encouraged to join the next MCX Plugtests event.

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 versions for the eighth MCX 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.

[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).

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

[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.

[40] ETSI TS 100 392-19-1: Interworking between TETRA and Broadband systems: Critical Communications Architecture for Interworking between TETRA and Broadband applications. (not published)

[41] ETSI TS 100 392-19-2: Interworking between TETRA and Broadband systems: Format for the transport of TETRA speech over mission critical broadband systems.

[42] TIA-102.BACA-B-3: Project 25 Inter-RF Subsystem Interface Messages and Procedures for Voice Services, Mobility Management, and RFSS Capability Polling Services.

[43] TIA-102.BACD-B-3: Inter-RF Subsystem Interface (ISSI) - Messages and Procedures for Supplementary Data.

[44] OMA. OMA-TS-REST-NetAPI-NMS-V1-0-20190528-C: RESTful Network API for Network Message Storage".

[45] OMA. OMA-TS-REST-NetAPI-NotificationChannel-V1-0-20200319-C: RESTful Network API for Notification Channel.

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
EUTC	European Utilities Telecom Council
FD	File Distribution
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
IWF	Interworking Function
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
OB_GW	On-Board Gateway
OTT	Over the Top
P25	Project 25
PCC	Policy and Charging Control
PCRF	Policy and Charging Rules Function
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
TETRA	Terrestrial Trunked Radio
TR	Technical Recommendation
TRT	Test Reporting Tool
TS	Technical Specification

TS-GW	Track-side Gateway
UE	User Equipment
UIC	International union of railways (Union Internationale des Chemins de fer)
UMA	University of Malaga

4. Technical and Project Management

4.1 Scope

The main goal of the eighth MCX Plugtests was testing the interoperability of the MCPTT, MCData and MCVideo ecosystem signalling and media plane at different levels. The railway related FRMCS functionalities, Off-Network and interworking (IWF) with LMR was also tested during the event.

The basic scenario tested comprised MCX application server(s) -both controlling and participating- and MCX clients deployed over a generic SIP/IMS core, LTE & 5G access network with and without MCX required PCC capabilities with native multicast support (i.e. Release-14 -and higher- eMBMS) and UEs. The following Figure 1 illustrates the basic test infrastructure. Additionally, off-network communications between two UEs using 5G sideling was evaluated.

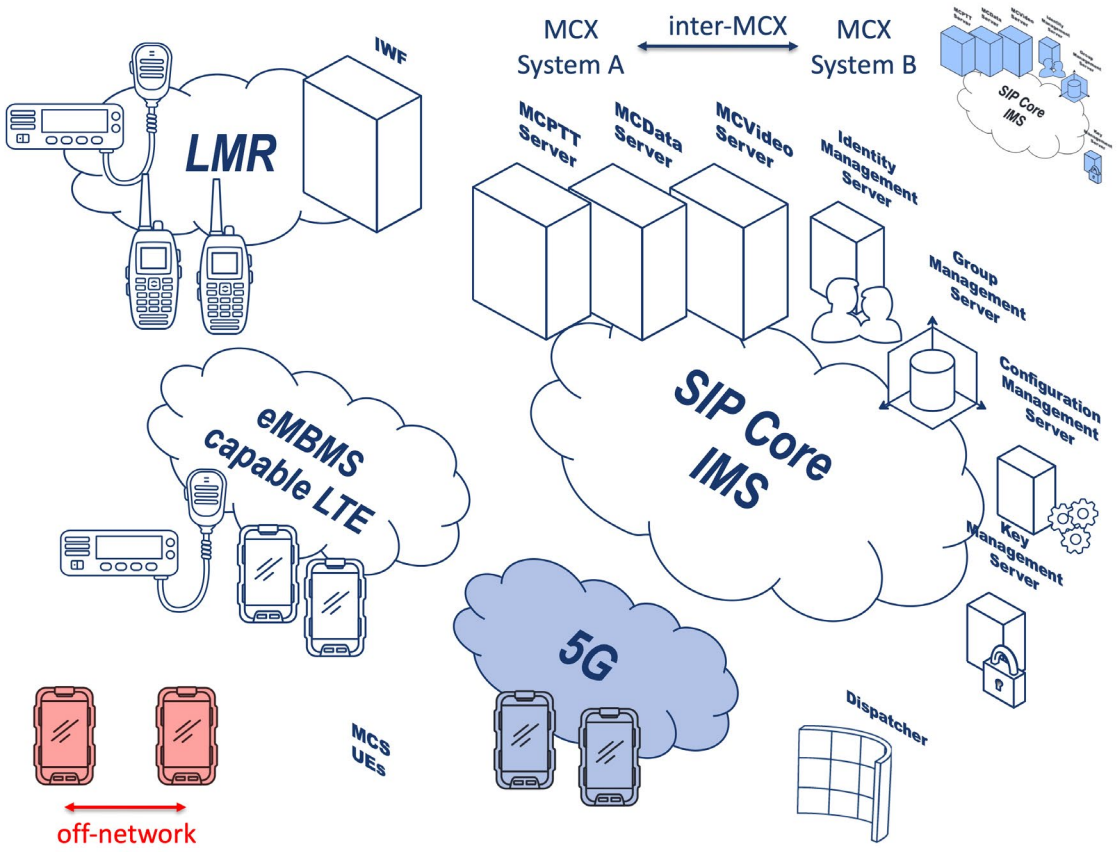

Figure 1. Typical MCPTT/MCData/MCVideo scenario to be considered in the Plugtests

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

- **Connectivity (CONN)**: Tests covered basic connectivity between functional elements at different levels including Access Network (LTE), IP Network, SIP/IMS and MCPTT/MCData/MCVideo Application level. At LTE level, unicast and more particularly eMBMS multicast connectivity was evaluated. Tests at IP layer targeted pure OTT connectivity regardless the underlying access network. SIP connectivity tests checked proper deployment of MCX AS over the selected SIP Core/IMS so that all SIP messages were successfully delivered from MCX Clients to Participating/Controlling MCPTT Servers and vice versa. In this 7th Plugtests, again, some AS vendors provided their own built in SIP/IMS cores so that Clients registered into different cores depending of the specific test session. Application level refers to e2e signalling, media, floor controlling (and other involved) protocols in use. Although for this Plugtests participants were encouraged to carry on CONN tests over Mission Critical LTE/5G for unicast – or UNI-MC-LTE/5G – and Mission Critical LTE/5G with multicast eMBMS-capabilities – so called MULTI-MC-LTE/5G -, most tests used the OTT (i.e. using WIFI / wired connections) one for its flexibility and the possibility of scheduling parallel test easily. Additionally, low level configuration-specific details (i.e. MCPTT. MC QCI and eMBMS bearer management) were considered in the PCC and eMBMS specific objectives. MCData and MCVideo features were mostly

analysed in test cases associated to the CONN objective while sibling procedures (i.e. registration to different MCPTT/MCData/MCVideo servers) were carried out when needed.

- **Floor Controlling (FC):** Apart from the basic Floor Controlling procedures considered during the first CONN objective, FC comprised comprehensive interoperability analysis of more complex interactions, including prioritization and pre-emptive mechanisms. Additional test cases comprising more advanced floor controlling (i.e. timeouts and revokes) were evaluated.
- **Policing (PCC)**: Comprised specific checking proper LTE dynamic bearer signalling and allocation by eUTRAN/EPC.
- **eMBMS (EMBMS)**: Comprised checking of eMBMS specific signalling both in the MB2-U/C interface and e2e.
- **Registration and authorization (REGAUTH)**: Comprised MCX Client registration.
- **Affiliation (AFFIL)**: Comprised MCX Client explicit and implicite affiliation
- **Location (LOC)**: In the test specification document several location configuration, retrieval and submission procedures were considered.
- **OAM procedures (CSC):** Comprised OAM related IdMS, CMS, GMS and KMS interfacing procedures. Mostly MCPTT mechanisms were evaluated since MCData/MCVideo implementations were not as mature as MCPTT implementations and are also mainly equivalent to MCPTT implementations.
- **Security (SEC):** Comprised security related procedures (including both signalling and media cyphering and key retrieval considered in KMS-related test cases in CSC test cases).
- **MCVideo Transmission Control (TC):** Traditional MCVideo call types and Transmission Control operations covered in previous Plugtests were newly evaluated. Several additional new MCVideo call types were also added for this plugtests.
- **Server-to-server communications (S2S)**: Controlling to non-controlling interface for temporary groups in different trust configurations.
- **FRMCS**: Railway oriented features were implemented to test functional aliases, IP Connectivity, etc.
- **MCData**: SDS and File Distribution mechanisms and newly added emergency alerting mechanisms.
- **IOP**: Interoperability testing oriented complex test cases were added.
- **Observer Test Scenarios**: more complex test scenarios which have been developed by observers.
- **Interworking Function (IWF)**: MCPTT connectivity test cases were re-used to test interworking with LMR systems (Tetra and P25).
- **Inter MCX**: MCPTT/MCVideo connectivity test cases were used to test interworking between application servers.
- **Off-Network:** MCPTT off network test cases were used to test direct mode communication using Sidelink UEs.

4.2 Timeline

The preparation was run through different phases as described in the Figure 2 below.

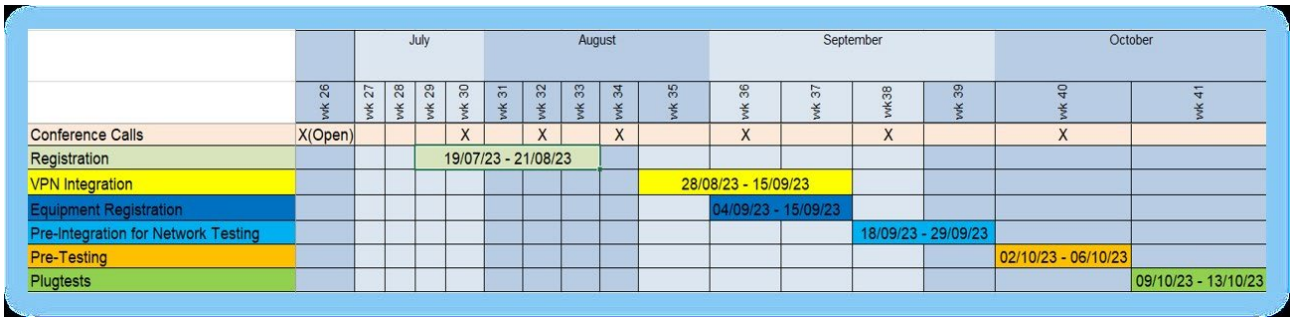

Figure 2. Plugtests event timeline

Registration to the MCX Plugtests event was open from 19th July 2023 to 21st August 2023 to any organisation willing to participate in testing the MCX Services Ecosystem. A total of 189 people were finally involved in the 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) 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 Specification Release-17 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, considering input and feedback received from Plugtests event participants. See details in clause 8.

4.2.2 Integration & pre-testing

Participants connected their implementations remotely to the Plugtests event infrastructure, known as HIVE: Hub for Interoperability and Validation at ETSI. Participants also integrated their equipment with University of Malaga LTE and 5G test networks to participate in the streams A, B and C.

From 18th September to 29th September 2023, participants connected their equipment's with UMA LTE and 5G network to collaboratively run the Interoperability Test Sessions remotely. Over the top IP based testing was performed during the pretesting phase from 02nd October to 07th October 2023.

During this phase, up to 30 remote labs connected to HIVE 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 the HIVE was highly recommended for participants providing MCX Application Servers, MCX Clients, Dispatchers, gNB and EPC 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.

For the LTE and 5G testing at the University of Malaga (UMA) in Spain, MCX AS Servers were connected to the UMA LTE and 5G test systems. Assistance was provided by the UMA experts to debug integration issues with the test networks.

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 09th October to 13th October 2023, participants connected their equipment's with UMA test network to collaboratively run the Interoperability Test Sessions remotely. Over the top IP based testing was also performed by some participants.

The scheduling of individual test combinations was partly done randomly using ETSI Test Reporting tool. Participants agreed test session slots between themselves. 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 MCX 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.
- **Host Information** – Information about the equipment available at host University of Malaga.
- **Visa Information** – Visa related information was provided for vendors require visa for travel.
- **List of Participants** – List of participants in the event.
- **Schedule –** Complete schedule of the event.
- **Observer Program** – Information about the Observer presentations and Observer demo during the Plugtests event.
- **Test Tools** – Information from the Test Tool vendors about what kind of tests they are offering for the Plugtests.
- **Test Network Information –** LTE and 5G test network information.
- **IT Infrastructure** - HIVE connection request tool, and remote connections status overview.
- **Specifications -** High Level Test Scope including the test specification and reference to 3GPP and IETF specifications.
- **Equipment under Test** - Participating EUTs overview and contact information.
- **Off-Network** – Information regarding sidelink UEs for port numbers/broadcast address.
- **Provisioning Information -** Pre-configured parameters for EUTs.
- **Test Reporting Tool** - Documentation of the Test Reporting Tool.
- **Conf 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.
- **Networking Dinner** – Information regarding networking dinner.
- **Shipment of Equipment** – Information regarding shipment of equipment.

In addition, Slack and Google Sheets 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.

5. Equipment Under Test

The tables Table 1 to Table 12 below summarise the different EUTs provided by the Plugtests event participants:

5.1 MCX Application Servers

Organisation	Support
Airbus	MCPTT, MCDATA, MCVIDEO
Alea	MCPTT, MCDATA, MCVIDEO, IWF
Aselsan	MCPTT, MCDATA, MCVIDEO
Consort Digital	MCPTT, MCDATA
Cybertel	MCPTT, MCDATA, MCVIDEO
Frequentis	MCPTT, MCDATA, MCVIDEO
HMF	MCPTT, MCDATA
Hytera	MCPTT, MCDATA, MCVIDEO, FRMCS
Kontron	MCPTT, MCDATA, FRMCS
MCLabs	MCPTT, MCDATA, MCVIDEO
Motorola	MCPTT, MCDATA, MCVIDEO, IWF
Nemergent	MCPTT, MCDATA, MCVIDEO, IWF
Samsung	MCPTT, MCDATA, MCVIDEO
StreamWide	MCPTT, MCDATA, MCVIDEO, IWF
TASSTA	MCPTT, MCDATA, MCVIDEO
Valid8	MCPTT, FRMCS

Table 1. MCX Application Servers Under Test

5.2 MCX Clients

Organisation	Support
Alea	MCPTT, MCDATA, MCVIDEO, OFF-Network
Alstom	MCDATA, FRMCS, ON BOARD GATEWAY, TRACK SIDE GATEWAY
Consort Digital	MCPTT, MCDATA
Eviden	MCPTT, MCDATA, MCVIDEO, FRMCS, IWF
Hytera	MCPTT, MCDATA, MCVIDEO, FRMCS
Kontron	MCPTT, MCDATA, FRMCS
MCLabs	MCPTT, MCVIDEO, FRMCS, OFF-NETWORK
Nemergent	MCPTT, MCDATA, MCVIDEO, IWF, OFF-NETWORK
Sepura	MCPTT
Softil	MCPTT, MCDATA, MCVIDEO, OFF-NETWORK
Tassta	MCPTT, MCDATA, MCVIDEO
Valid8	MCPTT, OFF-Network

Table 2. MCX Clients Under Test

5.3 Dispatcher (DISP)

Organisation	Support
Consort Digital	MCPTT, MCDATA
Eurofunk	MCPTT, MCDATA
Eviden	MCPTT, MCDATA, MCVIDEO
Frequentis	MCPTT, MCDATA, FRMCS
Kolibri	MCPTT, MCDATA
Kontron	MCPTT, MCDATA, FRMCS

Organisation	Support
Softil	MCPTT, MCDATA, MCVIDEO, FRMCS
Tassta	MCPTT, MCDATA, MCVIDEO
Teltronic	MCPTT, MCDATA, FRMCS
Zetron	MCPTT

Table 3. Dispatcher (DISP) Under Test

5.4 Evolved Packet Core (EPC)

Organisation	Support
Teltronic	
University of Malaga	Test system

Table 4. Evolved Packet Core Under Test

5.5 Evolved Node B (ENB)

Organisation	Support
Enensys	
Teltronic	
University of Malaga	Test system

Table 5. Evolved Node B Under Test

5.6 5G Core (5GC)

Organisation	Support
Athonet	

Table 6. 5G Core Under Test

5.7 5G New Radio (5GNR)

Organisation	Support
University of Malaga	Test system

Table 7. 5G NR Under Test

5.8 User Equipment (UE)

Organisation	Support
Alstom	4G, ON BOARD GATEWAY, TRACK SIDE GATEWAY
Aselsan	4G
Crosscall	4G, 5G NSA, 5G SA
Funkwerk	4G, 5G NSA, 5G SA
Hytera	4G, 5G NSA, 5G SA
Qualcomm	5G NR Sidelink
Sepura	4G

Table 8. User Equipment Under Test

5.9 Land Mobile Radio (LMR)

Organisation	Support
Eviden	LMR Simulator
Rohill	TETRA System

Table 9. Land Mobile Radio Under Test

5.10 Evolved Multimedia Broadcast Multicast Services (eMBMS) Components

Organisation	Support
Aselsan	
Enensys	
Teltronic	

Table 10. Evolved Multimedia Broadcast Multicast Services (eMBMS) Components Under Test

5.11 Cab Radio

Organisation	Support
Consort Digital	MCPTT, MCDATA
Teltronic	MCPTT, MCDATA

Table 11. Cabradio

5.12 Test Tools

Organisation	Support
MCS-TaaSting	MCX Conformance Tester
Valid8	MCX Conformance Tester

Table 12. 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 3:

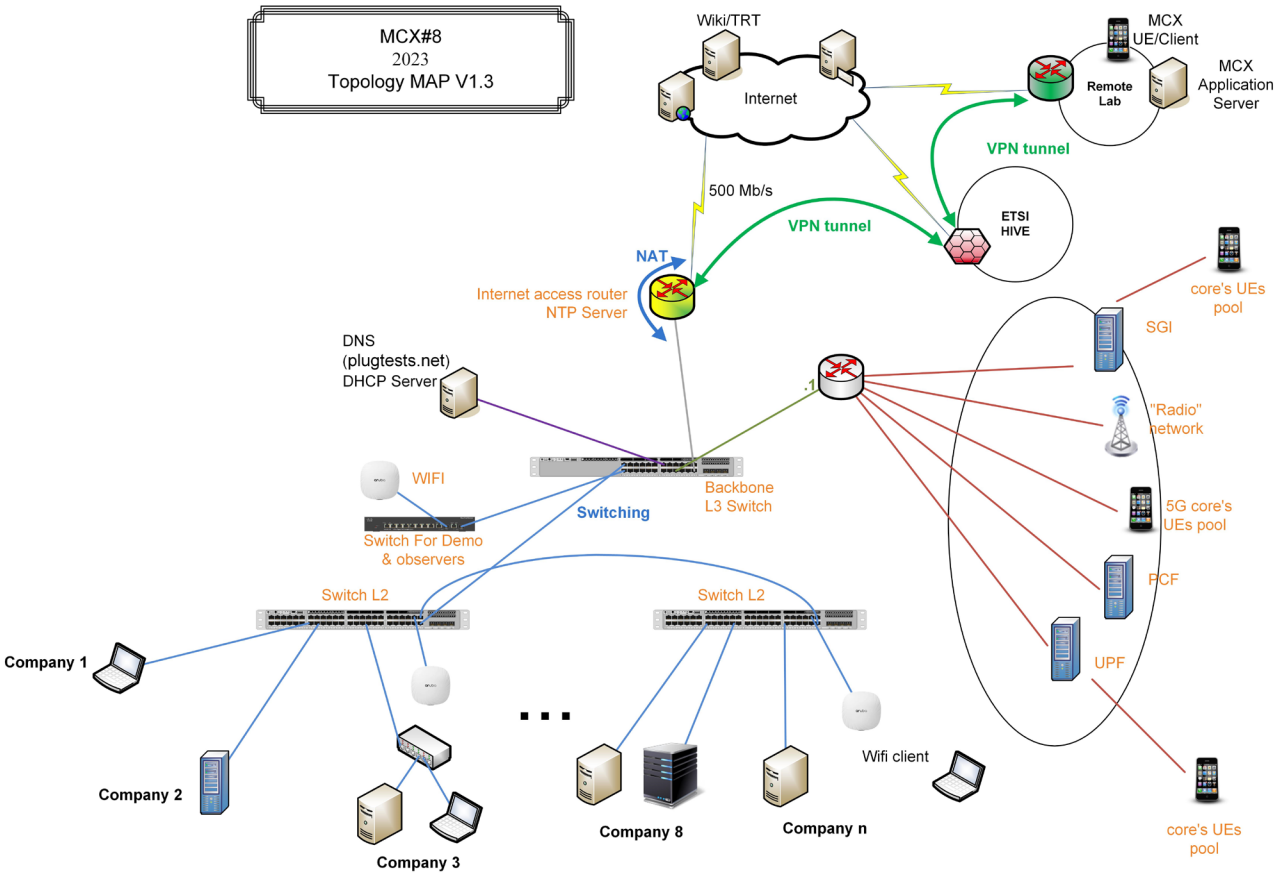

Figure 3. Remote Test Infrastructure

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 30 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 (see Table 13) were used in the pretesting phase.

Config Name	Pre-testing Configuration
Config Pre-test OTT	MCX Client + MCX AS
Config Pre-test IWF	MCX Client + MCX AS (P+C) + LMR
Config-Pretest-OTT-MBMS	MCX AS + BM-SC
Config-Pretest-OTT-CabRadio	MCX AS + CabRadio

Table 13. Pre-testing Configuration

7.2 Interoperability Testing Procedure

During the Plugtests event, a daily Test Session Schedule was added 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 (see Table 14).

Config Name	Main Test Configuration
Config-FRMCS	5GC + gNB + MCX Client + MCX AS (P+C) + 5G UE
Config-FRMCS-CabRadio	5GC + gNB + CabRadio + MCX AS (P+C)
Config-FRMCS-CabRadio-Disp	5GC + gNB + CabRadio + MCX AS (P+C) + Dispatcher
Config-MBMS	MCX Client + MCX AS (P+C) + 4G UE + eNB + EPC + MBMS GW + BM-SC
Config-MCX-4G	MCX Client + MCX AS (P+C) + 4G UE + eNB + EPC
Config-MCX-4G-CabRadio	CabRadio + MCX AS (P+C) + eNB + EPC
Config-MCX-4G-CabRadio-Disp	CabRadio + MCX AS (P+C) + eNB + EPC + Dispatcher
Config-MCX-4G-Disp	MCX Client + MCX AS (P+C) + 4G UE + eNB + EPC + Dispatcher
Config-MCX-4G-MultiClients-Disp	CabRadio + MCX Client + MCX AS (P+C) + 4G UE + eNB + EPC
Config-MCX-5G	MCX Client + MCX AS (P+C) + 5G UE + gNB + 5GC
Config-MCX-5G-CabRadio	CabRadio + MCX AS (P+C) + gNB + 5GC
Config-MCX-IWF	MCX Client + MCX AS (P+C) + 4G UE + eNB + EPC + LMR Tetra
Config-MCX-IWF-OTT	MCX Client + MCX AS (P+C) + LMR Tetra
Config-Off-Network	MCX Client + MCX Client + Sidelink UE + Sidelink UE
Config-Tester-AS	MCX Client + MCX AS
Config Tester Client	Tester + MCX Client
Config-Tester-LMR	LMR Tester + Tester

Table 14. 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.

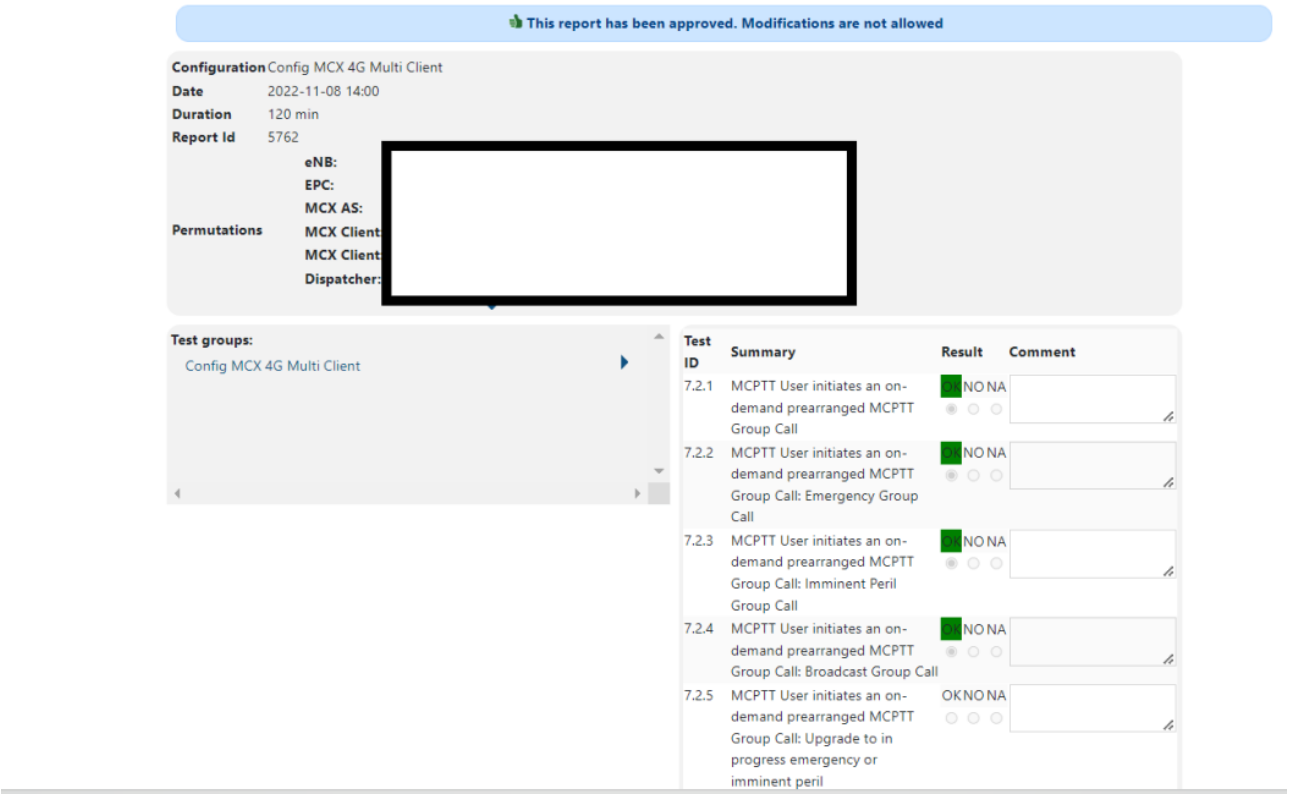

Figure 4. Test Session Report

2. For each Test in the Test Plan:

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

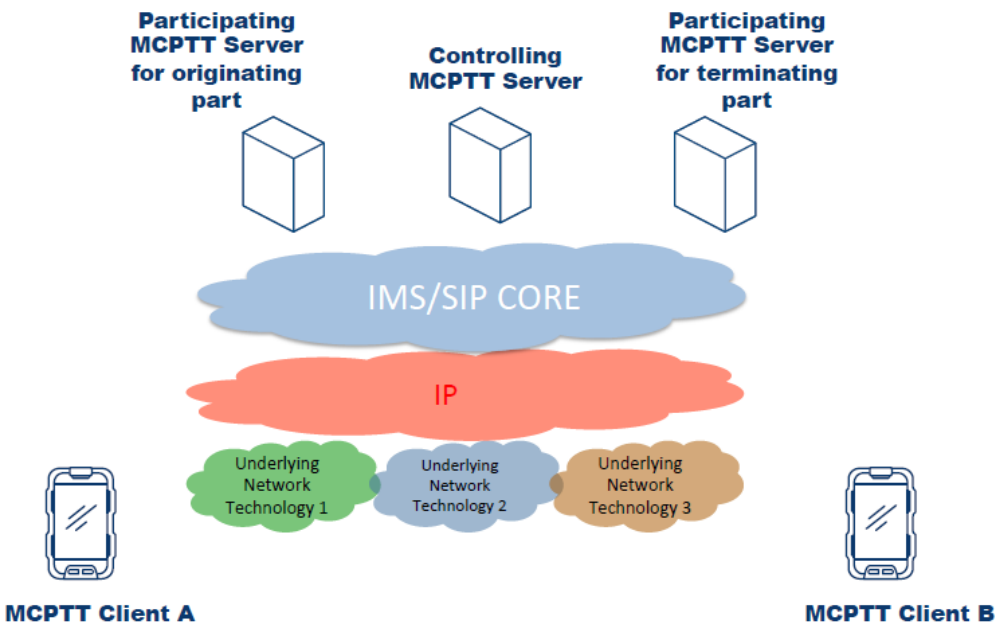

Figure 5. System Under Test (SUT) Configuration – MCPTT example

Interoperability Test Description			
Identifier	CONN/ONN/GROUP/PREA/ONDEM/NFC/01		
Test Objective	Verify IP connectivity, SIP core/IMS configuration and proper routing and SIP signaling of a pre-arranged on demand Group Call		
Configuration(s)	- CFG_ONN_OTT-1 (5.2) - CFG_ONN_UNI-MC-LTE-1 (5.3) - CFG_ONN_MULTI-MC-LTE-1 (5.4)		
References	- SIP (see [n.4] and other references in [n.5]) - MCPT (see [n.6] and other references in [n.5]) - RTP (see [n.4] and other references in [n.5])		
Applicability	- MCPTT-Client_ONN-MCPTT-CALL, MCPTT-Client_AMR-WB, MCPTT-Client_AFFIL, MCPTT-Client_MCPTT-FC (6.2) - MCPTT-Part_ONN-MCPTT-CALL, MCPTT-Part_AFFIL (see NOTE), MCPTT-Part_MCPTT-FC, MCPTT-Part_RX (CFG_ONN_UNI-MC-LTE-1 only), MCPTT-Part_GCSE (CFG_ONN_MULTI-MC-LTE-1 only), (6.5) - MCPTT-Ctrl_ONN-MCPTT-CALL, MCPTT-Ctrl_AFFIL (see NOTE) (6.6)		
Pre-test conditions	- IP connectivity among all elements of the specific scenario - Proper configuration of the SIP core/IMS to forward the signaling to the specific controlling and participating servers - UEs properly registered to the SIP core/IMS and MCPTT system - Calling user is affiliated to the called group		
Test Sequence	**Step**	**Type**	**Description**
	1	stimulus	User 1 (mcptt_id_clientA@example.com) calls mcptt-group-A
	2	check	Dialog creating INVITE received at the MCPTT participating server of mcptt_id_clientA@example.com after traversing SIP core/IMS
	3	check	INVITE received at the MCPTT controlling server
	4	check	The MCPTT controlling server loads the affiliated members of the mcptt-group-A (either preconfigured or retrieved from the GMS) and creates an INVITE per each of the "n" members
	5	check	"n" INVITEs received at the MCPTT participating servers of each mcptt_id_clientX (where X:1..n)
	6	check	"n" INVITEs received at the affiliated mcptt_id_clientX
	7	check	"n" SIP dialogs established
	8	verify	Call connected and multiple media flows exchanged

Figure 6. Test Description example

3. MCX 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 MCX equipment provider recorded the Test Result in the Test Session Report, as follows:

      i. OK: all IOP Checks were successful

      ii. NOK: 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 8th MCX Plugtests Test Plan was developed following ETSI guidelines for interoperability. Additional Release-17 based test cases were included comprising group regrouping, Inter MCX, MCData Message Store, Off Network and eMBMS.

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 MCX ecosystem comprises both controlling and participating MCPTT/MCData/MCVideo application server(s), MCPTT Clients deployed over a generic SIP Core/IMS, LTE/5G access network with and without MCPTT required PCC capabilities and native multicast support (i.e. Release-14 eMBMS). 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 Off-Network operations were also considered.

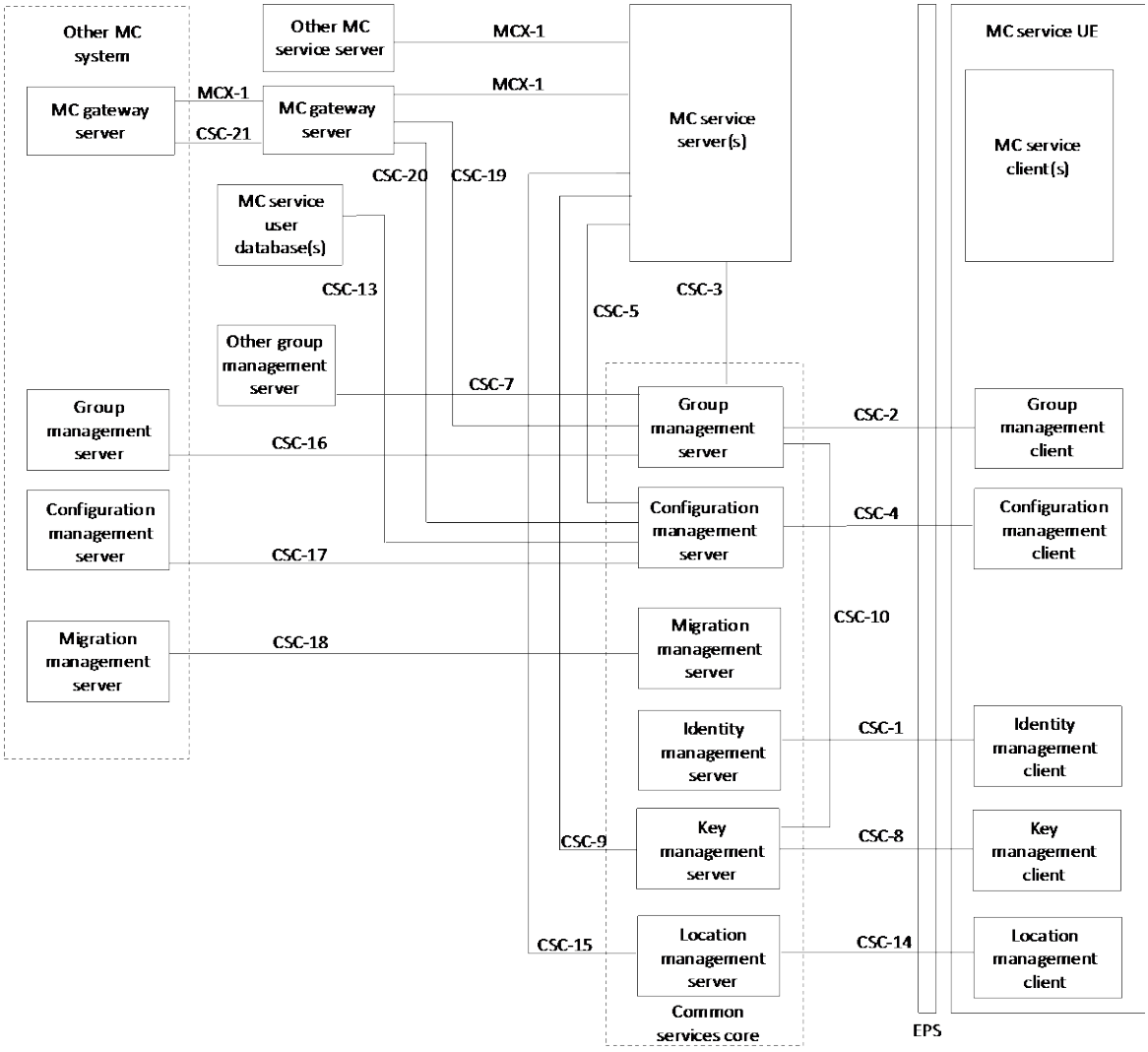

Figure 7. Functional model for on network application plane Figure 7.3.1-1 in 3GPP TS 23.280 [3]

Figure 8. Functional model for off network application plane Figure 7.3.2-1 in 3GPP TS 23.280 [3]

Figure 7.3.1-1 in 3GPP TS 23.280 [3] (see Figure 7) describes the overall architecture and the reference points considered for the interoperability testing for any (MCPTT/MCData/MCVideo) MC Service (MCS). As can be seen, the resulting number of functional elements, interfaces and protocols involved is quite large. Furthermore, there are MCPTT/MCData/MCVideo-only specific interfaces and others (like Rx/N5/N33 and MB2-C/MB2-U) involving other supporting technologies like LTE EPS, 5G, etc. In order to focus on MCS signalling the following three different configuration were initially considered: MCPTT/MCData/MCVideo as an application service over IP networks (Over-the-Top), unicast Mission Critical LTE/5G and multicast Mission Critical LTE/5G (all of them for On-Network calls only).

Similarly, Figure 7.3.2-1 in 3GPP TS 23.280 [3] (see Figure 8) describes the overall architecture and the reference points considered for the interoperability testing among MCS clients in off-network operations.

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/5G, 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/5G). 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/5G infrastructure and allowed both signalling and media plane parallel testing easily.

8.2.2 Unicast Mission Critical LTE/5G for On-Network calls (CFG_ONN_UNI-MC -1)

In this configuration the LTE network (both EPC and eUTRAN) and 5G network (both 5GC and gNB) 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 (or 5G Qi 65/69), 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 9, MCVideo/MCData could follow the same approach.

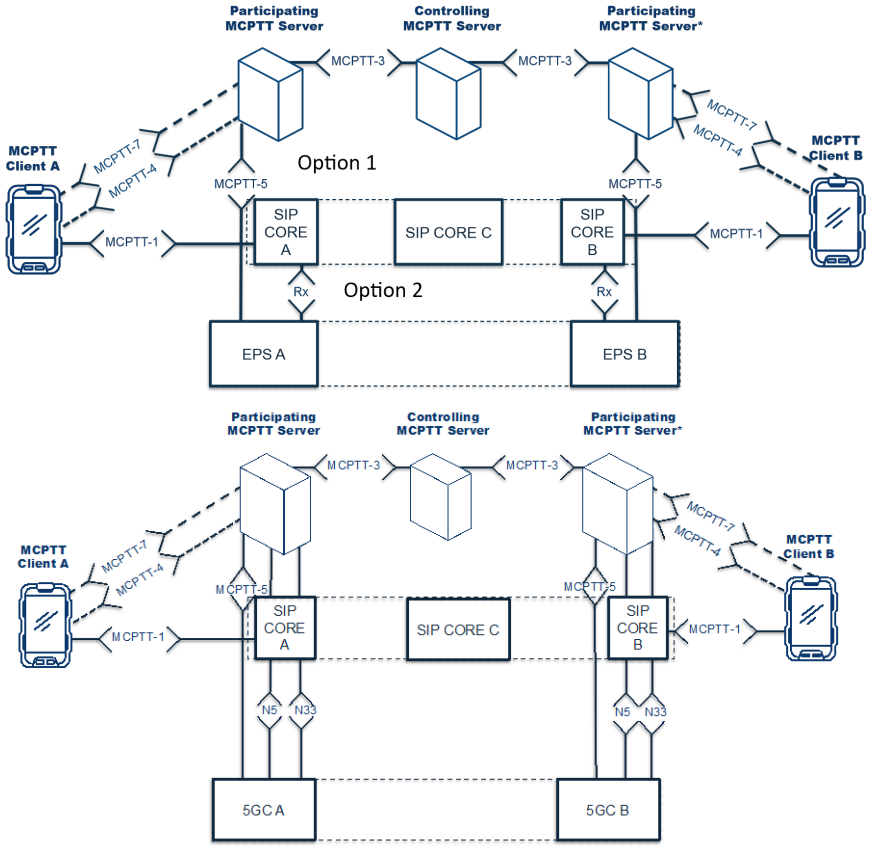

Figure 9. CFG_ONN_UNI-MC-LTE-1 configuration

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

In this configuration LTE/5G 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 8th MCX Plugtests both configurations (unicast and multicast scenarios) were possible.

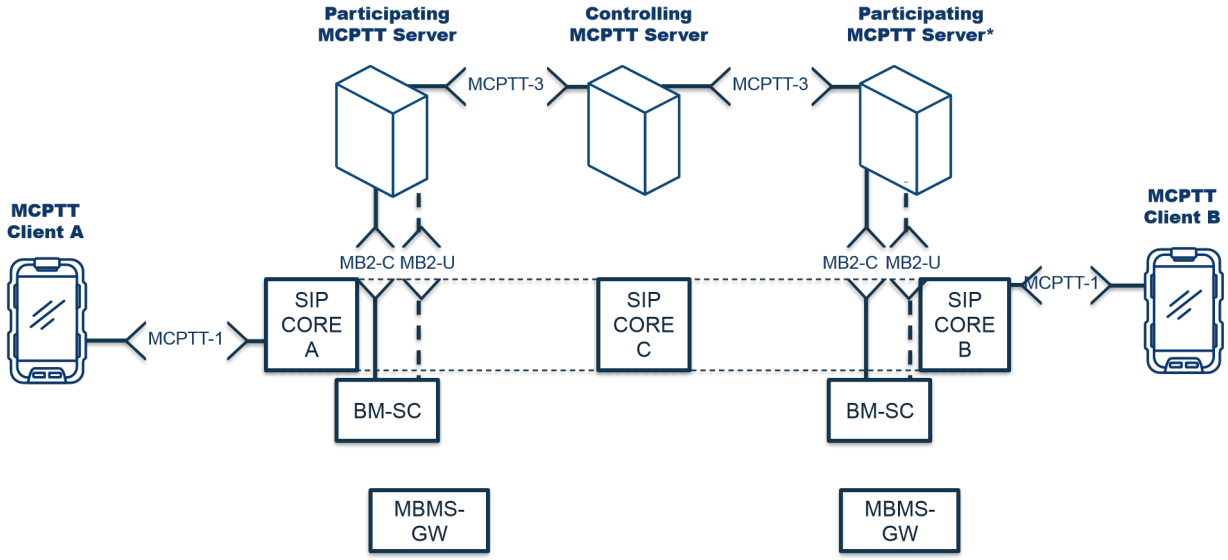

Figure 10. CFG_ONN_MULTI-MC-LTE-1 configuration

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-Pretest-OTT Config-MCX-IWF-OTT Config-Pretest-OTT-CabRadio Config-Pretest-OTT-MBMS
ONN-LTE	Config-MCX-4G Config-MBMS Config-MCX-4G-CabRadio Config-MCX-4G-CabRadio-Disp Config-MCX-4G-Disp Config-MCX-4G-MultiClients-Disp
ONN-5G	Config-MCX-5G Config-FRMCS Config-FRMCS-CabRadio Config-MCX-5G-CabRadio Config-FRMCS-CabRadio-Disp
ONN-OFF	Config-Off-Network

Table 15. Mapping of scenario architecture configurations and Plugtests event practical configurations

9 Interoperability Results

9.1 Overall Results

During the Plugtests event, a total of 179 Test Sessions were run: that is, 179 different combinations based on different configurations in Test Scope: MCX Client, MCX Server (Participating and Controlling), eNB, EPC, gNB, 5GC, LMR, Dispatcher, 4G UE, 5G UE, Sidelink UE and Testers were tested for interoperability. Overall, 1508 test executions were conducted and reported interoperability and conformance results.

Table 16 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.

Interoperability		Totals
PASS	**FAIL**	**Run**
1425 (94.5%)	83 (5.5%)	1508

Table 16. Overall Interoperability Results

Figure 11. Overall Interoperability results

A overall interoperability success rate of 94.5% 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

Table 17 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			
Configurations	**PASS**	**FAIL**	**Run**
Config-Pretest-OTT	703 (96.2%)	28 (3.8%)	731
Config-MCX-4G	300 (98.0%)	6 (2.0%)	306
Config-MCX-5G	73 (86.9%)	11 (13.1%)	84
Config-FRMCS	1 (100.0%)	0 (0.0%)	1
Config-MBMS	67 (100.0%)	0 (0.0%)	67
Config-Off-Network	7 (77.8%)	2 (22.2%)	9
Config-Tester-Client	6 (66.7%)	3 (33.3%)	9
Config-Tester-AS	3 (60.0%)	2 (40.0%)	5
Config-MCX-IWF-OTT	5 (100.0%)	0 (0.0%)	5
Config-FRMCS-CabRadio	0 (0.0%)	2 (100.0%)	2
Config-MCX-4G-CabRadio	0 (0.0%)	0 (0.0%)	0
Config-Pretest-OTT-CabRadio	56 (94.9%)	3 (5.1%)	59
Config-Pretest-OTT-MBMS	4 (80.0%)	1 (20.0%)	5
Config-MCX-4G-CabRadio-Disp	80 (93.0%)	6 (7.0%)	86
Config-MCX-IWF	17 (94.4%)	1 (5.6%)	18
Config-MCX-4G-Disp	59 (86.8%)	9 (13.2%)	68
Config-MCX-4G-MultiClients-Disp	22 (91.7%)	2 (8.3%)	24
Config-MCX-5G-CabRadio	16 (76.2%)	5 (23.8%)	21
Config-Tester-LMR	1 (100.0%)	0 (0.0%)	1
Config-FRMCS-CabRadio-Disp	5 (71.4%)	2 (28.6%)	7

Table 17. Results per Test Configuration

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

9.3 Successful Integrations

The following Figures Figure 12 to Figure 17 show the integrated equipments for each test stream. The grey lines show the initially planned integrations; the blue lines show the successful pre-integrations; and the green lines show the actual integrations which were used for the tests during the Plugtests week.

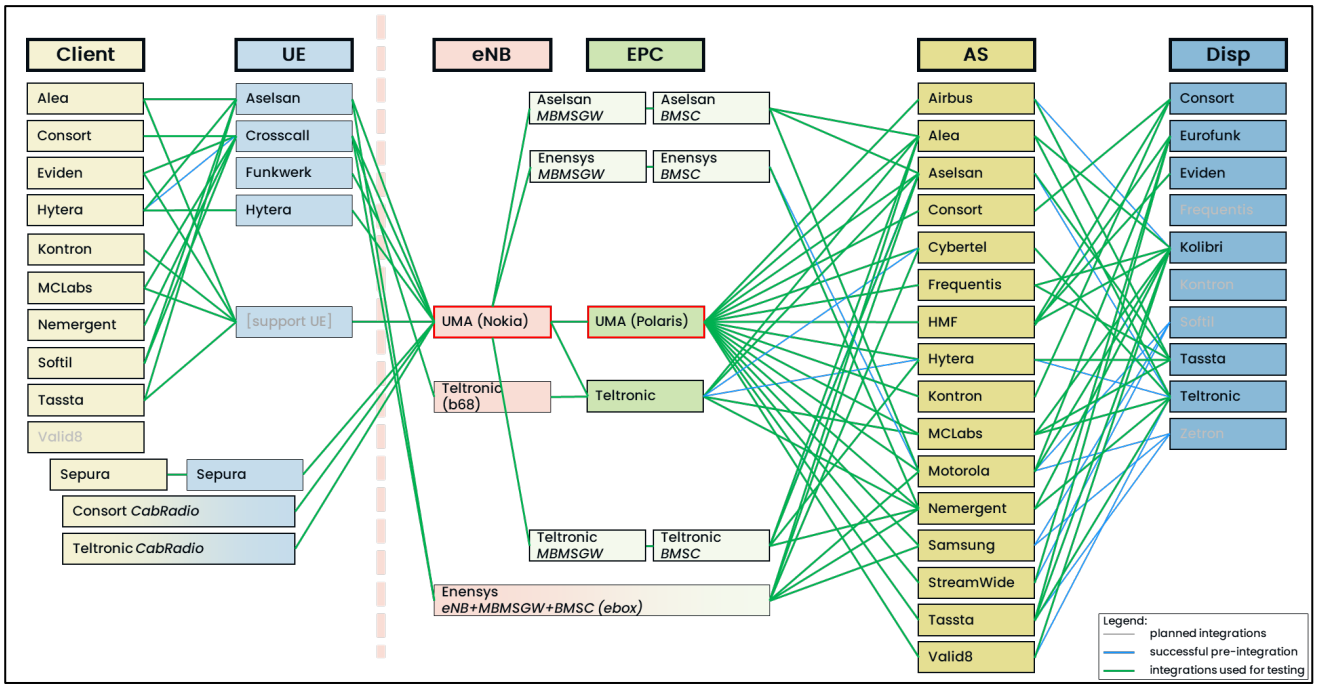

Figure 12. Tested Equipment for Stream A: MCX over 4G

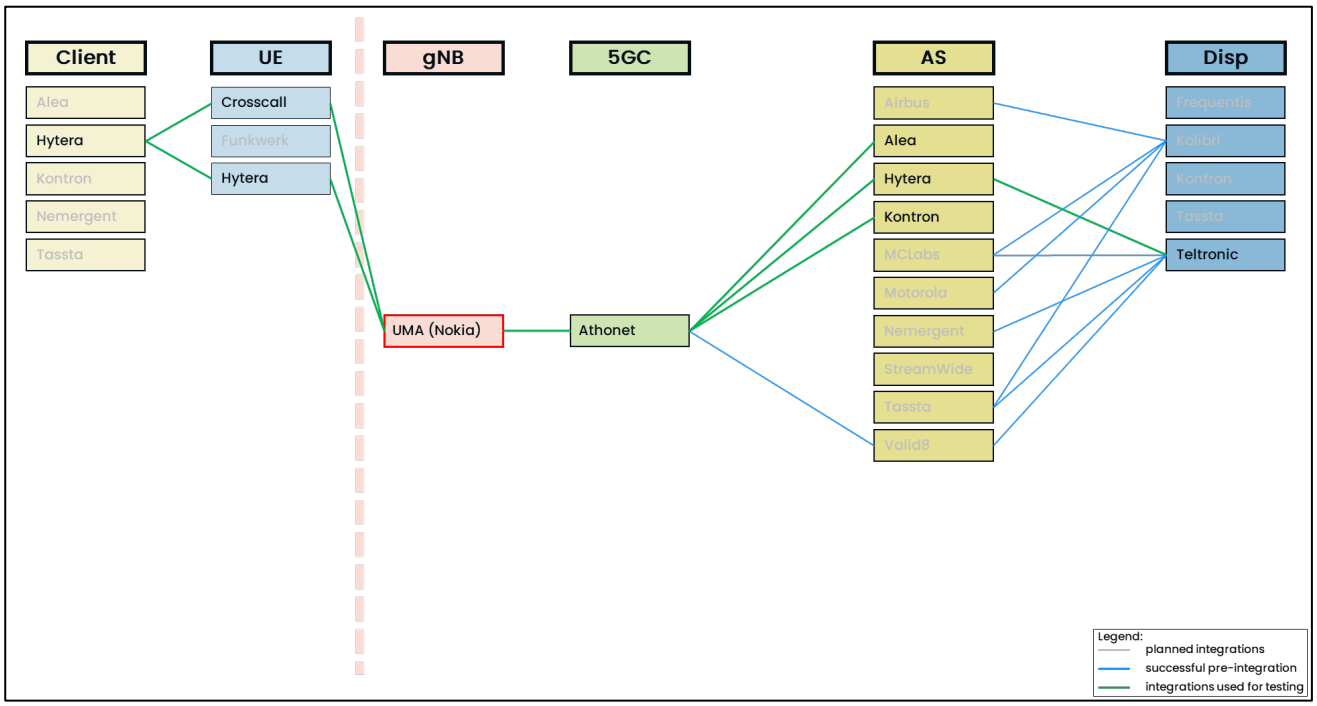

Figure 13. Tested Equipment for Stream B: MCX over 5G

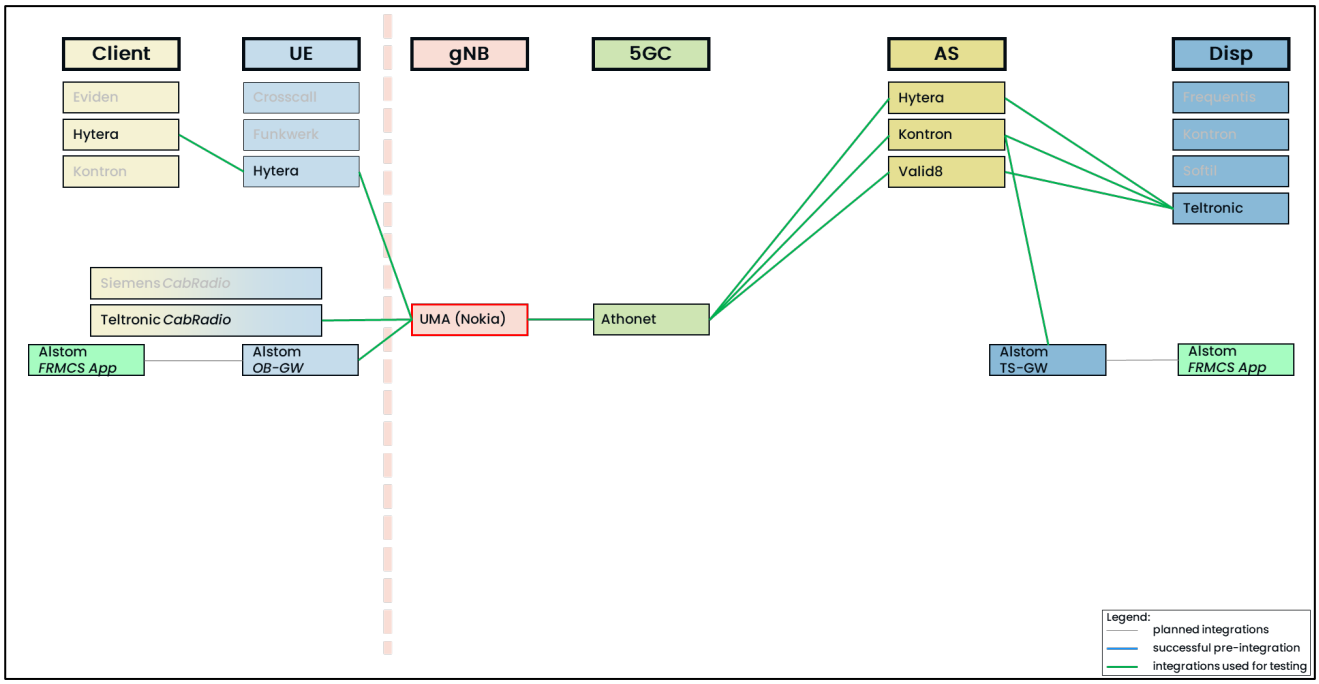

Figure 14. Tested Equipment for Stream C: FRMCS over 5G

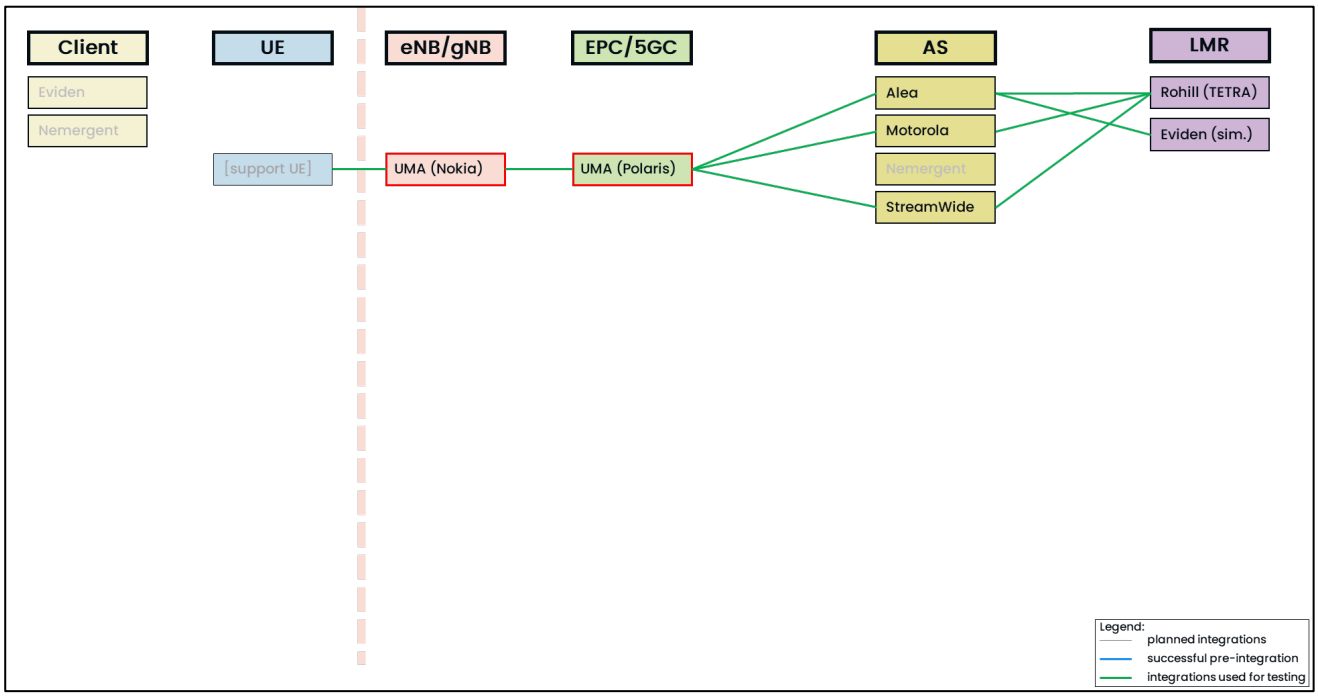

Figure 15. Tested Equipment for Stream D: Interworking with LMR

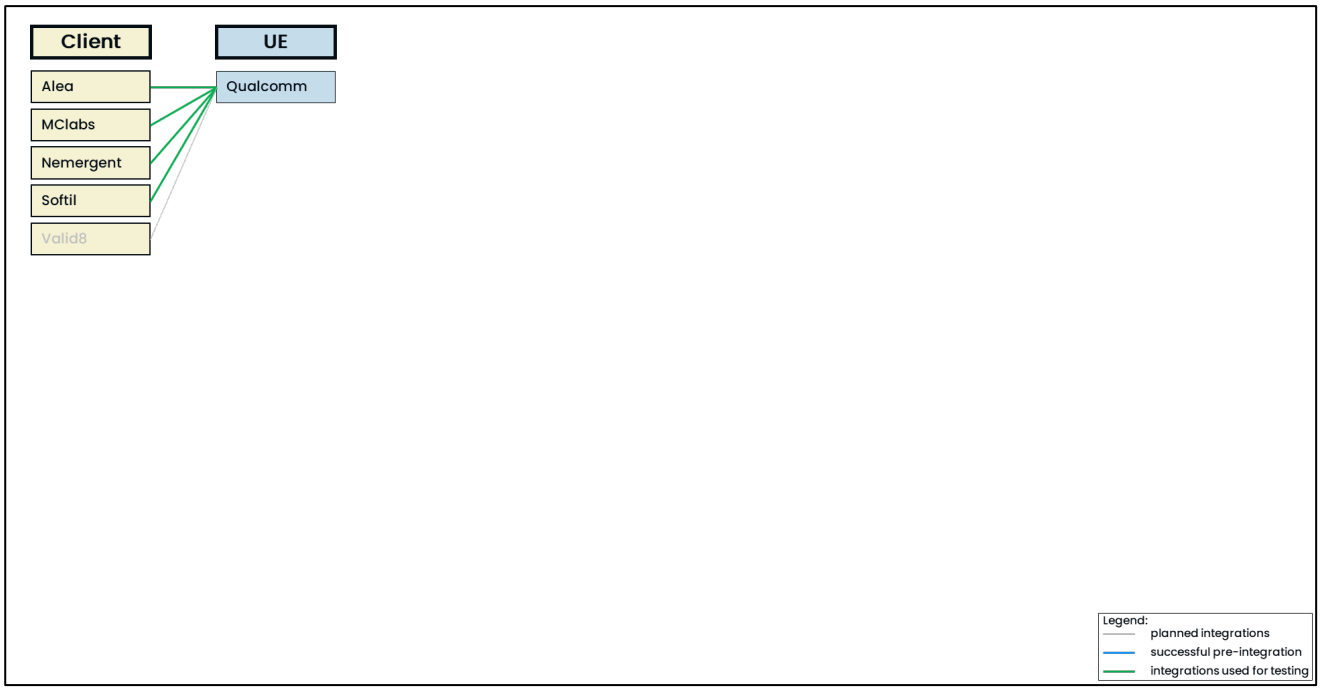

Figure 16. Tested Equipment for Stream E: Off-network

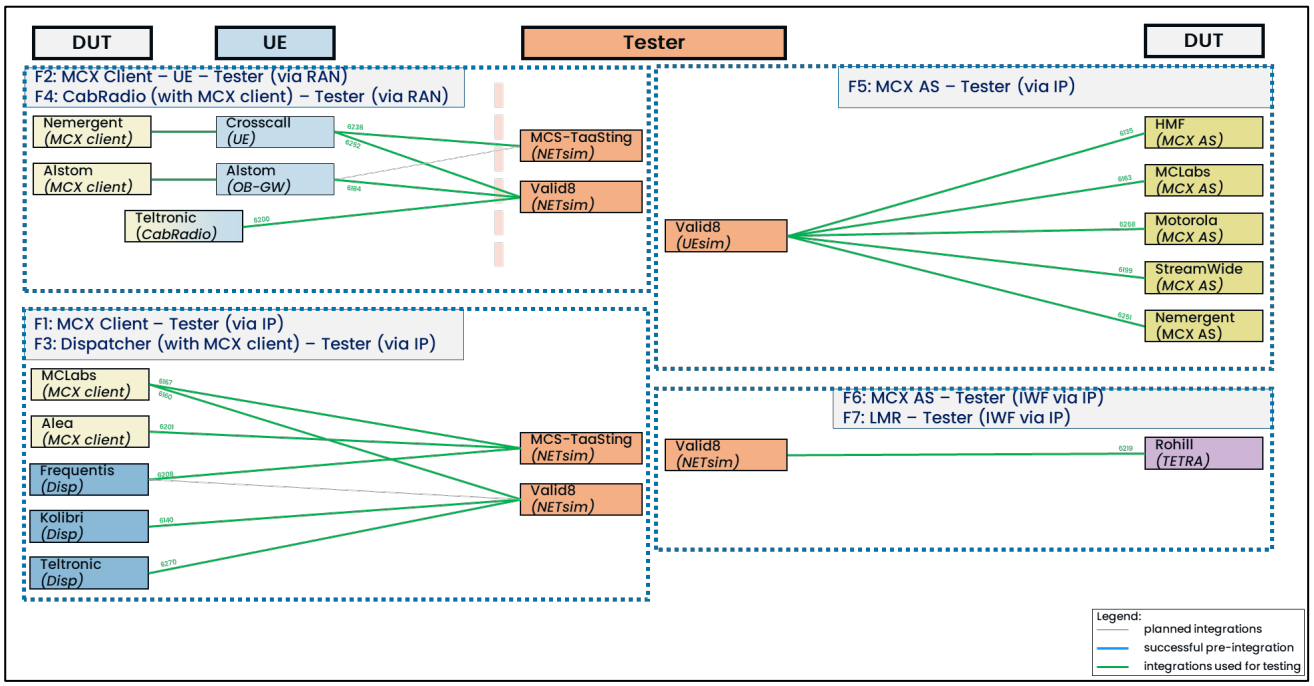

Figure 17. Tested Equipment for Stream F: Test Tools

9.4 Results per Test Case

Table 18 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.

Test Case #	Interoperability	
	PASS	FAIL
7.2.1	64 (94.1%)	4 (5.9%)
7.2.2	41 (95.3%)	2 (4.7%)
7.2.3	21 (91.3%)	2 (8.7%)
7.2.4	19 (95.0%)	1 (5.0%)
7.2.5	6 (85.7%)	1 (14.3%)
7.2.6	36 (100.0%)	0 (0.0%)
7.2.7	6 (75.0%)	2 (25.0%)
7.2.8	5 (100.0%)	0 (0.0%)
7.2.9	19 (95.0%)	1 (5.0%)
7.2.10	0 (0.0%)	1 (100.0%)
7.2.11	0 (0.0%)	0 (0.0%)
7.2.12	0 (0.0%)	0 (0.0%)
7.2.13	0 (0.0%)	0 (0.0%)
7.2.14	1 (100.0%)	0 (0.0%)
7.2.15	54 (93.1%)	4 (6.9%)
7.2.16	46 (93.9%)	3 (6.1%)
7.2.17	4 (100.0%)	0 (0.0%)
7.2.18	4 (100.0%)	0 (0.0%)
7.2.19	38 (95.0%)	2 (5.0%)
7.2.20	56 (96.6%)	2 (3.4%)
7.2.21	1 (100.0%)	0 (0.0%)
7.2.22	1 (50.0%)	1 (50.0%)
7.2.23	4 (100.0%)	0 (0.0%)
7.2.24	8 (100.0%)	0 (0.0%)
7.2.25	0 (0.0%)	0 (0.0%)
7.2.26	0 (0.0%)	0 (0.0%)
7.2.27	3 (60.0%)	2 (40.0%)
7.2.28	3 (100.0%)	0 (0.0%)
7.2.29	3 (100.0%)	0 (0.0%)
7.2.30	6 (85.7%)	1 (14.3%)
7.2.31	4 (100.0%)	0 (0.0%)
7.2.32	1 (100.0%)	0 (0.0%)
7.2.33	1 (100.0%)	0 (0.0%)
7.2.34	4 (100.0%)	0 (0.0%)
7.2.35	4 (100.0%)	0 (0.0%)
7.2.36	2 (100.0%)	0 (0.0%)
7.2.37	1 (100.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.2.38	0 (0.0%)	0 (0.0%)
7.2.39	20 (83.3%)	4 (16.7%)
7.2.40	0 (0.0%)	0 (0.0%)
7.2.41	0 (0.0%)	0 (0.0%)
7.2.42	17 (89.5%)	2 (10.5%)
7.2.43	0 (0.0%)	0 (0.0%)
7.2.44	0 (0.0%)	0 (0.0%)
7.2.45	0 (0.0%)	0 (0.0%)
7.2.46	1 (100.0%)	0 (0.0%)
7.2.47	0 (0.0%)	0 (0.0%)
7.2.48	0 (0.0%)	0 (0.0%)
7.2.49	9 (90.0%)	1 (10.0%)
7.2.50	8 (88.9%)	1 (11.1%)
7.2.51	0 (0.0%)	0 (0.0%)
7.2.52	0 (0.0%)	0 (0.0%)
7.2.53	0 (0.0%)	0 (0.0%)
7.2.54	1 (100.0%)	0 (0.0%)
7.2.55	4 (100.0%)	0 (0.0%)
7.2.56	5 (100.0%)	0 (0.0%)
7.2.57	3 (75.0%)	1 (25.0%)
7.2.58	9 (100.0%)	0 (0.0%)
7.2.59	1 (100.0%)	0 (0.0%)
7.2.60	10 (90.9%)	1 (9.1%)
7.2.61	0 (0.0%)	0 (0.0%)
7.2.62	2 (66.7%)	1 (33.3%)
7.2.63	24 (88.9%)	3 (11.1%)
7.2.64	5 (83.3%)	1 (16.7%)
7.2.65	6 (85.7%)	1 (14.3%)
7.2.66	1 (100.0%)	0 (0.0%)
7.2.67	2 (100.0%)	0 (0.0%)
7.2.68	2 (100.0%)	0 (0.0%)
7.2.69	5 (100.0%)	0 (0.0%)
7.2.70	0 (0.0%)	0 (0.0%)
7.2.71	0 (0.0%)	0 (0.0%)
7.2.72	0 (0.0%)	0 (0.0%)
7.2.73	4 (80.0%)	1 (20.0%)
7.2.74	0 (0.0%)	0 (0.0%)
7.2.75	0 (0.0%)	0 (0.0%)
7.2.76	0 (0.0%)	0 (0.0%)
7.2.77	0 (0.0%)	0 (0.0%)
7.2.78	1 (100.0%)	0 (0.0%)
7.2.79	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.2.80	0 (0.0%)	0 (0.0%)
7.2.81	0 (0.0%)	0 (0.0%)
7.2.82	3 (100.0%)	0 (0.0%)
7.2.83	4 (100.0%)	0 (0.0%)
7.2.84	2 (100.0%)	0 (0.0%)
7.2.85	1 (50.0%)	1 (50.0%)
7.2.86	0 (0.0%)	0 (0.0%)
7.2.87	0 (0.0%)	0 (0.0%)
7.2.88	0 (0.0%)	0 (0.0%)
7.2.89	0 (0.0%)	0 (0.0%)
7.2.90	0 (0.0%)	0 (0.0%)
7.2.91	0 (0.0%)	0 (0.0%)
7.2.92	0 (0.0%)	0 (0.0%)
7.2.93	0 (0.0%)	0 (0.0%)
7.2.94	0 (0.0%)	0 (0.0%)
7.2.95	0 (0.0%)	0 (0.0%)
7.2.96	0 (0.0%)	0 (0.0%)
7.2.97	0 (0.0%)	0 (0.0%)
7.2.98	0 (0.0%)	0 (0.0%)
7.2.99	0 (0.0%)	0 (0.0%)
7.2.100	0 (0.0%)	0 (0.0%)
7.2.101	0 (0.0%)	0 (0.0%)
7.2.102	1 (100.0%)	0 (0.0%)
7.2.103	5 (100.0%)	0 (0.0%)
7.2.104	8 (100.0%)	0 (0.0%)
7.2.105	0 (0.0%)	0 (0.0%)
7.2.106	0 (0.0%)	0 (0.0%)
7.2.107	1 (100.0%)	0 (0.0%)
7.2.108	1 (100.0%)	0 (0.0%)
7.2.109	0 (0.0%)	0 (0.0%)
7.2.110	0 (0.0%)	0 (0.0%)
7.2.111	1 (100.0%)	0 (0.0%)
7.2.112	1 (100.0%)	0 (0.0%)
7.2.113	0 (0.0%)	0 (0.0%)
7.2.114	0 (0.0%)	0 (0.0%)
7.2.115	0 (0.0%)	0 (0.0%)
7.2.116	0 (0.0%)	0 (0.0%)
7.2.117	0 (0.0%)	0 (0.0%)
7.2.118	0 (0.0%)	0 (0.0%)
7.2.119	0 (0.0%)	0 (0.0%)
7.2.120	2 (66.7%)	1 (33.3%)
7.2.121	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.2.122	1 (100.0%)	0 (0.0%)
7.2.123	1 (100.0%)	0 (0.0%)
7.2.124	1 (100.0%)	0 (0.0%)
7.2.125	0 (0.0%)	0 (0.0%)
7.2.126	0 (0.0%)	0 (0.0%)
7.2.127	0 (0.0%)	0 (0.0%)
7.2.128	2 (100.0%)	0 (0.0%)
7.2.129	2 (100.0%)	0 (0.0%)
7.2.130	2 (100.0%)	0 (0.0%)
7.2.131	0 (0.0%)	0 (0.0%)
7.2.132	0 (0.0%)	0 (0.0%)
7.3.1	60 (96.8%)	2 (3.2%)
7.3.2	3 (75.0%)	1 (25.0%)
7.3.3	17 (94.4%)	1 (5.6%)
7.3.4	13 (92.9%)	1 (7.1%)
7.3.5	6 (100.0%)	0 (0.0%)
7.3.6	1 (100.0%)	0 (0.0%)
7.3.7	1 (100.0%)	0 (0.0%)
7.3.8	0 (0.0%)	0 (0.0%)
7.3.9	0 (0.0%)	0 (0.0%)
7.4.1	59 (95.2%)	3 (4.8%)
7.4.2	85 (96.6%)	3 (3.4%)
7.4.3	73 (94.8%)	4 (5.2%)
7.4.4	1 (100.0%)	0 (0.0%)
7.4.5	0 (0.0%)	0 (0.0%)
7.5.1	1 (100.0%)	0 (0.0%)
7.5.2	2 (100.0%)	0 (0.0%)
7.5.3	0 (0.0%)	0 (0.0%)
7.5.4	0 (0.0%)	0 (0.0%)
7.5.5	0 (0.0%)	0 (0.0%)
7.5.6	0 (0.0%)	0 (0.0%)
7.5.7	0 (0.0%)	0 (0.0%)
7.5.8	0 (0.0%)	0 (0.0%)
7.5.9	0 (0.0%)	0 (0.0%)
7.5.10	1 (100.0%)	0 (0.0%)
7.5.11	0 (0.0%)	0 (0.0%)
7.5.12	0 (0.0%)	0 (0.0%)
7.5.13	0 (0.0%)	0 (0.0%)
7.5.14	0 (0.0%)	0 (0.0%)
7.5.15	0 (0.0%)	0 (0.0%)
7.5.16	0 (0.0%)	0 (0.0%)
7.5.15	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.5.16	0 (0.0%)	0 (0.0%)
7.5.17	0 (0.0%)	0 (0.0%)
7.5.18	0 (0.0%)	0 (0.0%)
7.6.2	5 (100.0%)	0 (0.0%)
7.6.3	6 (100.0%)	0 (0.0%)
7.6.4	2 (100.0%)	0 (0.0%)
7.6.5	1 (100.0%)	0 (0.0%)
7.6.6	1 (100.0%)	0 (0.0%)
7.6.7	3 (100.0%)	0 (0.0%)
7.6.8	4 (100.0%)	0 (0.0%)
7.6.9	0 (0.0%)	0 (0.0%)
7.6.10	3 (100.0%)	0 (0.0%)
7.6.11	0 (0.0%)	0 (0.0%)
7.6.12	0 (0.0%)	0 (0.0%)
7.6.13	0 (0.0%)	0 (0.0%)
7.6.14	0 (0.0%)	0 (0.0%)
7.6.15	1 (100.0%)	0 (0.0%)
7.6.16	0 (0.0%)	0 (0.0%)
7.6.17	0 (0.0%)	0 (0.0%)
7.6.18	0 (0.0%)	0 (0.0%)
7.6.19	0 (0.0%)	0 (0.0%)
7.6.20	1 (100.0%)	0 (0.0%)
7.6.21	0 (0.0%)	0 (0.0%)
7.7.1	84 (98.8%)	1 (1.2%)
7.7.2	17 (100.0%)	0 (0.0%)
7.7.3	62 (93.9%)	4 (6.1%)
7.7.4	5 (100.0%)	0 (0.0%)
7.7.5	1 (50.0%)	1 (50.0%)
7.7.6	3 (100.0%)	0 (0.0%)
7.7.7	3 (100.0%)	0 (0.0%)
7.7.8	0 (0.0%)	0 (0.0%)
7.7.9	1 (100.0%)	0 (0.0%)
7.8.1	8 (100.0%)	0 (0.0%)
7.8.2	2 (100.0%)	0 (0.0%)
7.8.3	6 (100.0%)	0 (0.0%)
7.9.1	11 (100.0%)	0 (0.0%)
7.9.2	13 (100.0%)	0 (0.0%)
7.9.3	13 (100.0%)	0 (0.0%)
7.9.4	4 (100.0%)	0 (0.0%)
7.9.5	10 (100.0%)	0 (0.0%)
7.9.6	4 (100.0%)	0 (0.0%)
7.9.7	4 (100.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.9.8	4 (100.0%)	0 (0.0%)
7.9.9	1 (100.0%)	0 (0.0%)
7.9.10	0 (0.0%)	0 (0.0%)
7.9.11	0 (0.0%)	0 (0.0%)
7.10.1	3 (100.0%)	0 (0.0%)
7.10.2	0 (0.0%)	0 (0.0%)
7.10.3	0 (0.0%)	0 (0.0%)
7.10.4	5 (100.0%)	0 (0.0%)
7.10.5	0 (0.0%)	0 (0.0%)
7.10.6	4 (100.0%)	0 (0.0%)
7.10.7	0 (0.0%)	0 (0.0%)
7.10.8	1 (100.0%)	0 (0.0%)
7.10.9	0 (0.0%)	0 (0.0%)
7.10.10	1 (100.0%)	0 (0.0%)
7.10.11	1 (100.0%)	0 (0.0%)
7.10.12	0 (0.0%)	0 (0.0%)
7.10.13	0 (0.0%)	0 (0.0%)
7.10.14	0 (0.0%)	0 (0.0%)
7.10.15	0 (0.0%)	0 (0.0%)
7.10.16	0 (0.0%)	0 (0.0%)
7.10.17	0 (0.0%)	0 (0.0%)
7.11.1	6 (75.0%)	2 (25.0%)
7.11.2	0 (0.0%)	0 (0.0%)
7.11.3	0 (0.0%)	0 (0.0%)
7.11.4	0 (0.0%)	0 (0.0%)
7.12.1	0 (0.0%)	0 (0.0%)
7.12.2	0 (0.0%)	0 (0.0%)
7.13.1	17 (94.4%)	1 (5.6%)
7.13.2	13 (100.0%)	0 (0.0%)
7.13.3	2 (100.0%)	0 (0.0%)
7.13.4	1 (100.0%)	0 (0.0%)
7.13.5	6 (100.0%)	0 (0.0%)
7.13.6	6 (100.0%)	0 (0.0%)
7.13.7	10 (83.3%)	2 (16.7%)
7.13.8	3 (100.0%)	0 (0.0%)
7.13.9	0 (0.0%)	0 (0.0%)
7.13.10	1 (100.0%)	0 (0.0%)
7.14.1	0 (0.0%)	0 (0.0%)
7.14.2	0 (0.0%)	0 (0.0%)
7.14.3	0 (0.0%)	0 (0.0%)
7.14.4	0 (0.0%)	0 (0.0%)
7.14.5	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
7.14.6	0 (0.0%)	0 (0.0%)
7.14.7	0 (0.0%)	0 (0.0%)
7.15.1	0 (0.0%)	0 (0.0%)
7.15.2	0 (0.0%)	0 (0.0%)
7.15.3	0 (0.0%)	0 (0.0%)
7.15.4	0 (0.0%)	0 (0.0%)
7.16.1	0 (0.0%)	0 (0.0%)
7.16.2	0 (0.0%)	0 (0.0%)
7.16.3	0 (0.0%)	0 (0.0%)
7.16.4	0 (0.0%)	0 (0.0%)
7.16.5	0 (0.0%)	0 (0.0%)
7.16.6	0 (0.0%)	0 (0.0%)
7.16.7	0 (0.0%)	0 (0.0%)
7.16.8	0 (0.0%)	0 (0.0%)
7.16.9	0 (0.0%)	0 (0.0%)
7.16.10	0 (0.0%)	0 (0.0%)
7.16.11	0 (0.0%)	0 (0.0%)
7.16.12	0 (0.0%)	0 (0.0%)
7.16.13	0 (0.0%)	0 (0.0%)
7.16.14	0 (0.0%)	0 (0.0%)
7.16.15	0 (0.0%)	0 (0.0%)
7.16.16	0 (0.0%)	0 (0.0%)
7.16.17	0 (0.0%)	0 (0.0%)
7.16.18	0 (0.0%)	0 (0.0%)
7.16.19	0 (0.0%)	0 (0.0%)
7.16.20	0 (0.0%)	0 (0.0%)
7.16.21	0 (0.0%)	0 (0.0%)
7.16.22	0 (0.0%)	0 (0.0%)
8.2.1	10 (100.0%)	0 (0.0%)
8.2.2	8 (88.9%)	1 (11.1%)
8.2.3	13 (100.0%)	0 (0.0%)
8.2.4	9 (100.0%)	0 (0.0%)
8.2.5	0 (0.0%)	0 (0.0%)
8.2.6	0 (0.0%)	0 (0.0%)
8.2.7	0 (0.0%)	0 (0.0%)
8.2.8	0 (0.0%)	0 (0.0%)
8.2.9	0 (0.0%)	0 (0.0%)
8.2.10	0 (0.0%)	0 (0.0%)
8.2.11	0 (0.0%)	0 (0.0%)
8.2.12	2 (100.0%)	0 (0.0%)
8.2.13	0 (0.0%)	0 (0.0%)
8.2.14	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
8.2.15	0 (0.0%)	0 (0.0%)
8.2.16	0 (0.0%)	0 (0.0%)
8.2.17	0 (0.0%)	0 (0.0%)
8.2.18	3 (100.0%)	0 (0.0%)
8.2.19	0 (0.0%)	0 (0.0%)
9.3	4 (100.0%)	0 (0.0%)
9.4	4 (100.0%)	0 (0.0%)
9.5	0 (0.0%)	0 (0.0%)
9.6	0 (0.0%)	0 (0.0%)
9.7	0 (0.0%)	0 (0.0%)
9.8	0 (0.0%)	0 (0.0%)
9.9	0 (0.0%)	0 (0.0%)
9.10	0 (0.0%)	0 (0.0%)
9.11	1 (100.0%)	0 (0.0%)
9.12	0 (0.0%)	0 (0.0%)
9.13	0 (0.0%)	0 (0.0%)
9.14	0 (0.0%)	0 (0.0%)
10.5	0 (0.0%)	0 (0.0%)
10.6	0 (0.0%)	0 (0.0%)
10.7	0 (0.0%)	0 (0.0%)
10.8	0 (0.0%)	0 (0.0%)
10.9	0 (0.0%)	0 (0.0%)
10.10	1 (100.0%)	0 (0.0%)
10.11	0 (0.0%)	0 (0.0%)
10.12	0 (0.0%)	0 (0.0%)
11.2.1	2 (100.0%)	0 (0.0%)
11.2.2	0 (0.0%)	0 (0.0%)
11.2.3	0 (0.0%)	0 (0.0%)
11.2.4	0 (0.0%)	0 (0.0%)
11.2.5	0 (0.0%)	0 (0.0%)
11.3.1	4 (80.0%)	1 (20.0%)
11.3.2	0 (0.0%)	0 (0.0%)
11.3.3	0 (0.0%)	0 (0.0%)
11.3.4	4 (100.0%)	0 (0.0%)
11.3.5	0 (0.0%)	0 (0.0%)
11.3.6	0 (0.0%)	0 (0.0%)
11.3.7	0 (0.0%)	0 (0.0%)
11.3.8	0 (0.0%)	0 (0.0%)
11.3.9	1 (100.0%)	0 (0.0%)
11.3.10	1 (100.0%)	0 (0.0%)
11.3.11	0 (0.0%)	0 (0.0%)
11.3.12	0 (0.0%)	0 (0.0%)

Test Case #	Interoperability	
	PASS	FAIL
11.3.13	1 (100.0%)	0 (0.0%)
11.3.14	1 (100.0%)	0 (0.0%)
11.3.15	0 (0.0%)	0 (0.0%)
11.3.16	0 (0.0%)	0 (0.0%)
11.3.17	0 (0.0%)	0 (0.0%)
11.3.18	0 (0.0%)	0 (0.0%)
11.3.19	1 (100.0%)	0 (0.0%)
11.3.20	2 (100.0%)	0 (0.0%)
11.3.21	2 (100.0%)	0 (0.0%)
11.3.22	2 (100.0%)	0 (0.0%)
11.3.23	1 (100.0%)	0 (0.0%)
11.3.24	0 (0.0%)	0 (0.0%)
11.3.25	0 (0.0%)	0 (0.0%)
11.3.26	0 (0.0%)	0 (0.0%)
11.4.1	0 (0.0%)	0 (0.0%)
11.4.2	0 (0.0%)	0 (0.0%)
12.2.2	0 (0.0%)	0 (0.0%)
12.2.3	0 (0.0%)	0 (0.0%)
12.2.4	0 (0.0%)	0 (0.0%)
12.2.5	0 (0.0%)	0 (0.0%)
12.2.6	0 (0.0%)	0 (0.0%)
12.3.2	0 (0.0%)	0 (0.0%)
12.3.3	0 (0.0%)	0 (0.0%)
12.3.4	0 (0.0%)	0 (0.0%)
12.3.5	0 (0.0%)	0 (0.0%)
12.3.6	0 (0.0%)	0 (0.0%)
13.2.1	3 (100.0%)	0 (0.0%)
13.2.2	0 (0.0%)	1 (100.0%)
13.2.3	2 (100.0%)	0 (0.0%)
13.2.4	2 (100.0%)	0 (0.0%)
13.2.5	0 (0.0%)	0 (0.0%)
13.2.6	0 (0.0%)	0 (0.0%)
13.2.7	0 (0.0%)	1 (100.0%)
13.2.8	0 (0.0%)	0 (0.0%)
Conformance Testing	10 (66.7%)	5 (33.3%)

Table 18. 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 MCX vendors in most deployments.

The reader should note that 3GPP Release 17 was considered for the eighth MCX Plugtests event.

The 8th MCX 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 Observations

10.1.1 Unclear usage of "Inviting MCPTT User Identity" in the MCPC Connect or reINVITES to identify the callee in first-to-answer calls over pre-established sessions

Clause 8.3.3.7 in 3GPP TS 24.380 defines the format and overall meaning for the "Inviting MCPTT User Identity" as "the inviting MCPTT user". Although this definition covers most of the MCPC procedures for many call types, the value for first-to-answer call is unclear.

10.1.2 Group keys update [Request for clarification]

Assuming that group keys shall follow an update scheme similar to the one of RFC 6509, section 3.3, then near the start of each key period clients have to receive both old key material and new key material.

In particular, RFC 6509 states in 3.3. that "Implementations MUST allow devices to hold two periods' keys simultaneously to allow for differences in system time between the Initiator and Responder". Since 3GPP TS 24.481 in Clause 7.7.4.2 allows more than one GKTP element per group:

```
<xs:complexType name="singleTypeGKTPsType">
  <xs:sequence>
    <xs:element name="GKTP" type="mgktp:GKTPType" minOccurs="0" maxOccurs="unbounded"/>
    ...
  </xs:sequence>
  ...
</xs:complexType>
```

there is a request regarding whether it is correct to include 2 GKTP elements per group in the NOTIFY near the start of a key period, one with old key material and one with new key material.

10.1.3 KMS keys update [Request for clarification]

Similarly to the previous Observation, RFC 6509 states in 3.3 that KMSs MAY update their KMS Master Secret Keys and KMS Master Secret Authentication Keys. If such an update is not deemed necessary, then the corresponding KMS Public Keys and KMS Public Authentication Keys will be fixed. If KMS keys are to be updated, then this update MUST occur at the change of a key period, and new KMS Public Key(s) and KMS Public Authentication Key(s) MUST be provided to all users with their user key material.

The same paragraph also states that "Implementations MUST allow devices to hold two periods' keys simultaneously to allow for differences in system time between the Initiator and Responder"

Within MCS specification (3GPP TS 33.180, Clause D.2.3) KMS public keys are obtained via a HTTP POST request to /keymanagement/identity/v1/init, So that, a) there is no time parameter in the Request-Uri and b) there is a time

parameter in the body of the request, but it's the time of the request, not an arbitrary time (as in 3GPP TS 33.180 Clause D.2.2).

Thus it's not clear how a client or service would be able to obtain KMS public keys from 2 different key periods and a clarification is requested to confirm that MCS specification support the update of KMS keys and, in the case it does, es, how do clients and services obtain both the old and the new KMS public keys near the start of a key period.

10.1.4 CSK upload with SIP REGISTER [Request for clarification]

The CSK upload procedure (3GPP TS 33.180, Clause 9.2.1.3) mandates that the CSK is included in the initial SIP REGISTER or SIP PUBLISH request in a MIKEY message within an application/mikey payload. However, the initial SIP REGISTER may contain more than one service identity, i.e. MCPTT, MCData, MCVideo identities and access tokens for each service identity are included in service specific payloads, i.e. application/vnd.3gpp.mcptt-info+xml, application/vnd.3gpp.mcdata-info+xml, application/vnd.3gpp.mcvideo-info+xml. Therefore, since application/mikey is not a service specific payload and can contain only one MIKEY, Plugtests participants would like to request for clarification whether/how it is possible to include multiple MIKEY messages (one per service) in the same SIP REGISTER.

10.1.5 Emergency alert notification after affiliation

When a member of a (pre-arranged) group starts an emergency alert all other members of this group are notified of this new alert state by means of a SIP MESSAGE request (3GPP TS 24.379, Clause 12.1.3.1 4bii). When another client subsequently affiliates to that group, according to the specs, it will not receive any notification of the existing emergency alert state. This means different group members can have a different view of the group's emergency alert state.

As a solution, Plugtests participants propose that newly affiliated group members should be notified of an existing emergency alert state of that group, preferably by means of a SIP MESSAGE request.

10.1.6 Behaviour upon receiving CALL PROBE from a new UE under off-network coverage during an ongoing group call [Request for clarification]

ETSI TS 103.564 (draft) TC 13.4 illustrates the situation when a new client triggers an off-network group call to the same group call ID already involved in an ongoing one. Upon receiving the GROUP CALL PROBE all the clients already involved in one (state S3) seem to simply ignore the CALL PROBE (according to 10.2.2.4.2.3 in 3GPP TS 24.379) so that the "late join"-ing one should need to wait anyway for the periodic group call announcement as in 10.2.2.4.3.2 to realize there is an ongoing group call and passively join the call. Relevant 3GPP WG (CT1) is kindly request to clarify whether this behavior is intentional or otherwise another response should be triggered.

10.1.7 Unspecified procedures for Floor Indicator bits

Clause 8.2.3.15 in 3GPP TS 24.380 specifies meanings for the bits in the Floor Indicator Field, e.g. Normal call (bit A), Emergency call (bit D).

However NOTE 1 states "The indicators A, B, C, D and E are only informative. There are no procedures specified for the A, B, C, D and E indicators in this release of the present document but they can be used to provide information to the user about type of call."

Some server vendors indicate value 32,768 for a normal call (only bit A set to 1) and value 4,096 for an emergency call (only bit D set to 1). However, some other server vendors indicate e.g. value 36,864 for an emergency call (both bit A and bit D set to 1), or even e.g. value 65,408 (all bits A to I set to 1, all bits J to P set to 0), which can result in clients (and logging tools) interpreting these combinations as an unknown state and blocking the sending of floor requests in emergency calls.

The final paragraph states "There can be more than one bit set to 1 at the same time. The local policy in the floor control server decides which combinations are possible and the priority of the indications."

As a proposed solution, for the sake of interoperability, TS 24.380 section 8.2.3.15 should specify explicitly which combinations of bits are valid, and how they are to be interpreted. Preferably only one of bits A to E should be set to 1.

10.1.8 Dispatchers (MCx clients) unable to request location of other MCx clients [NOTE]

Some Plugtests Participants requested feedback regarding the availability of Stage 3 procedures to enable requesting location from the so-called location management servers (CSC-14).

10.1.9 Missing MCData functionality for dispatchers [NOTE]

Similarly to previous observations some Dispatching solutions vendors claimed that unlike other environments such as TETRA and DMR, MCData specifications may miss some functionality such as location configuration and retrieval, indoor location.

10.1.10 Encoding and formatting of MCData [NOTE]

As part of the 3rd FRMCS plugtests an observation was made concerning the encoding of DATA Payload Text in TS 24.282. Especially the lack of possibility to specify the used encoding in the sent text message. Additionally 3GPP TS 24.282 contains more data types for which the need exists to know how they were encoded. Examples of these are hyperlinks and enhanced status in the Payload information element (15.2.13) and Organization Name (15.2.26).

Some pieces of information are encoded and/or formatted differently in different contexts and can contain more or less information. This lack of uniformity could lead to implementation mistakes and therefore hamper interoperability between vendors. As an example, location information is specified in different capacities, and with different pieces of information, in 15.2.13 Payload, 15.2.25 User location and Annex D4 XML, so that the Plugtests participant noted that similar solution to be agreed for text Payload could be extended to those.

10.1.11 Emergency state handling

Additional details: Use of unknown emergency state values

Table G.10-1 in TS 24.379 defines, amongst others, values 'MEPP 3: cancel-pending' and 'MEPP 4: confirm-pending' for MCPTT emergency private priority state. In the following Clauses the (unknown) value 'MEPP 3: confirm-pending' is used:

6.2.8.1.18
6.2.8.3.2
6.2.8.3.5
11.1.1.2.1.1
11.1.1.2.2.1

Similarly, values 'MEG 3: confirm-pending' and 'MIG 3: confirm-pending' are used in section 6.2.8.1.17 but not defined in table G.3-1 and G.7-1 respectively.

A minor observation is that table G.8-1 defines value 'MIGC 1: imminent peril-gc-capable', but value 'MIGC 1: imminent-peril-capable' is used in sections 6.2.8.1.4, 6.2.8.1.13 and 6.2.8.1.17.

Additional details: Wrong state referenced

Clause 6.2.8.1.9 of TS 24.379 handles the origination of an imminent peril group call by the client. Bullet point 1) references 'the in-progress emergency state of the group'. According to section G.2 this state is managed by the controlling MCPTT function and therefore not known to the MCPTT client. Also, the 'MIGC1' state is an MCPTT client imminent peril group call state.

Additional details: Cancel imminent peril group state when no group call exists

Clause 10.1.1.2.1.5 of TS 24.379 handles canceling the in-progress imminent peril condition of a prearranged group. The client is to send a SIP re-INVITE for the on-demand or pre-established session. It is unclear what the client should do when it uses on-demand sessions but no prearranged group call exists.

Additional details: Missing reset of MCPTT emergency group call state

After an MCPTT client has successfully set up an emergency group call the MCPTT emergency group call state will be 'MEGC 3: emergency-call-granted' (TS 24.379 Clause 6.2.8.1.4). When the call gets ended this state will not be changed, according to Clause 6.2.8.1.17. Also, when the client subsequently cancels the in-progress emergency condition of the group (12.1.1.5), this state remains the same. This means the MCPTT emergency group call state will never return to 'MEGC 1: emergency-gc-capable'3GPP would be kindly requested to consider the following actions for every observation details:

Use of unknown emergency state values

Check the actual value on every Clause.

Wrong state referenced

Change bullet 1) in Clause 6.2.8.1.9 in such a way that the MCPTT client emergency group state's value is checked instead of the in-progress emergency state. Additionally, add 'call' between 'group' and 'state'.

Cancel imminent peril group state when no group call exists

The TS should specify the action the client should take in this situation. This will most likely be similar to the action in clause10.1.1.2.1.4: send a SIP MESSAGE as specified in Clause 12.1.1.5. If so, please bear in mind that Clause 12.1.1.5 currently only handles canceling the in-progress emergency state and not the in-progress imminent peril state.

Missing reset of MCPTT emergency group call state

In TS 24.379 Clause 12.1.1.5, paragraph handling received SIP MESSAGE with <emergency-ind-rcvd>=true, bullet 1: add sub-bullet b) 'shall set the MCPTT emergency group call state of the group to "MEGC 1: emergency-gc-capable".'.

This would make it similar to Clause12.1.1.2. Another, possibly better, approach could be to reset the call state when the call has been ended, in Clause 6.2.8.1.17.

11 Observer Program

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

11.1 Preparation Phase

During equipment registration, interested vendors provided their intention to showcase during the observer demo. Test cases from ETSI TS 103 564 were used for the observer demo.

11.2 Observer Presentations

Observer presentation during MCX Plugtests event 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. The speakers were from government organisations, operators, regulators, users, associations which provide updates on deployment plans in their respective countries, pilot projects and updates on standards.
The observer program was conducted during half a day on 10th October 2023. The speakers presented to program outlined in Table 19.
Presentations in the observer program and the Questions & Answers are available on the Plugtests WIKI.

Presentations included:

Moderator – Hans Petter Naper / DSB

Program	Name/Organisation	Allocated Time
Welcome and Agenda	Hans Petter Naper / DSB	09:20 - 09:30
Update on TCCA Activities	Tero Pesonen / TCCA	09:30 - 09:50
Innovations for the Next Generation Digitalfunk - News on the BDBOS funding program	Philipp Hasbach / BDBOS	09:50 - 10:10
MCX Conformance Testing Challenges with Security Approaches	Harald Ludwig & Jeremy Wright / TCCA & Keysight	10:10 - 10:30
Status of the TCCA & GCF activities for MCX Certification	Harald Ludwig & Carlos Pedraz Rodríguez/ TCCA & GCF	10:30 - 11:00
Coffee Break – 30 mins		
How flow control over QCI 69 can improve MCPTT performance	Nathan Jeyaratnarajah / UK Home Office	11:30 - 11:50
GSMA MCX Roaming Task Force	Renaud Mellies / French MOI	11:50 - 12:10
Status on IWF and Use of Interconnection /Migration	Michel Duits / DSB	12:10 - 12:30
MCX Off Network	Walt Magnussen & Raja Sattiraju / TAMU ITEC & Qualcomm	12:30 - 12:50
Lunch - 13:00 to 14:00		

Table 19.Observer Program

11.3 Observer Round Table Discussion

Observer round table discussions were organised on 11th October 2023 during MCX Plugtests event which focused on sharing of ideas and strategies for testing mission critical networks and the eco-system.
Some of the topics discussed during the roundtable discussion are:

- Stages of PPDR certification
- Architecture and technology around implementation and transition of services from best practice systems to Mission Critical Services (MCS)
- How to reap the BB PPDR benefits by developing smart and useful data services on top of MCX.
- MCX Plugtests future funding
- Current stance of PPDR network providers concerning broadband D2D (Sidelink/Proximity Services/Applications, other infrastructure services) communications
- Funding of MCBB services
- GCF Phase 2 Work Item Prioritisation Survey
- PPDR networks interoperability => PPDR roaming

11.4 Observer Demos

The Observer Demo was a possibility for vendors to present their solutions and features to the observers. The demos took place during the 12th October 2023. The demos shown in Table 20 were presented:

Demo no.	Time	Participants	Test Cases
#1	09:00 – 09:20	Alea, Qualcomm, Softil	13.2.1, 13.2.3, 13.2.4
#3	09:25 – 09:45	Motorola, Zetron	7.2.32, 7.2.33, 7.2.36, 7.2.37, 7.2.128, 7.2.129, 7.2.130
#13	09:50 – 10:10	Crosscall, Frequentis, Funkwerk, Nemergent	7.13.1, 7.13.2, 7.2.5, 7.2.15, 7.2.16, 7.15.1, 7.15.2, 7.15.3, 7.15.4, 7.5.2
#5	10:15 – 10:35	Alea, Crosscall, Rohill	11.3.1, 11.3.4, 11.3.7, 11.3.9, 11.3.13, 11.3.20
#7	11:25 – 11:45	Crosscall, Nemergent, Teltronic	7.2.103, 7.2.104, 7.13.1, 7.13.2, 7.2.1, 7.6.3, 8.2.1, 8.2.3
#8	11:50 – 12:10	Athonet, Cybertel, Teltronic	7.2.2, 7.2.3, 7.2.27, 7.2.28, 7.2.29, 7.2.39, 7.2.42
#9	12:15– 12:35	Crosscall, Eviden, MClabs, Teltronic,	10.5, 7.5.1
#10	14:00 – 14:20	Rohill, Valid8	11.3.4
#14	14:25 – 14:45	Crosscall, Enensys, Motorola, Softil	7.2.7, 7.5.6, 8.2.3, 8.2.4, 7.6.4, 7.2.54, 7.2.56

Table 20. Observer Demos

12 History

Document history		
V0.0.0	18/10/2023	First Draft
V0.0.1	26/10/2023	Stable Draft
V0.0.2	06/11/2023	Stable Draft with corrections
V0.0.3	10/11/2023	Minor corrections in integrations
V1.0.0	13/11/2023	Final Draft
V1.1.0	13/11/2023	Report Published