MCX in Public Safety

EVOLVING STANDARDS AND INFRASTRUCTURE FOR ENHANCED PUBLIC SAFETY COMMUNICATIONS

MCX in Public Safety

Version: 4.0
Publication date: 13/11/2024
Status of the document: FINAL

Authors that contributed to this document:

Iratxe Gomez Susaeta, Eviden & Co-chair of Tech&Ops Comm.

Cristina Lumbreras, EENA

Freddie McBride, EENA

Ross Venhuizen, Motorola Solutions & Vice-chair of Tech&Ops Comm.

Wolfgang Kamplicher, Frequentis & Co-chair of Tech&Ops Comm.

Michael Proestler, Gridgears & Vice-chair of Tech&Ops Comm.

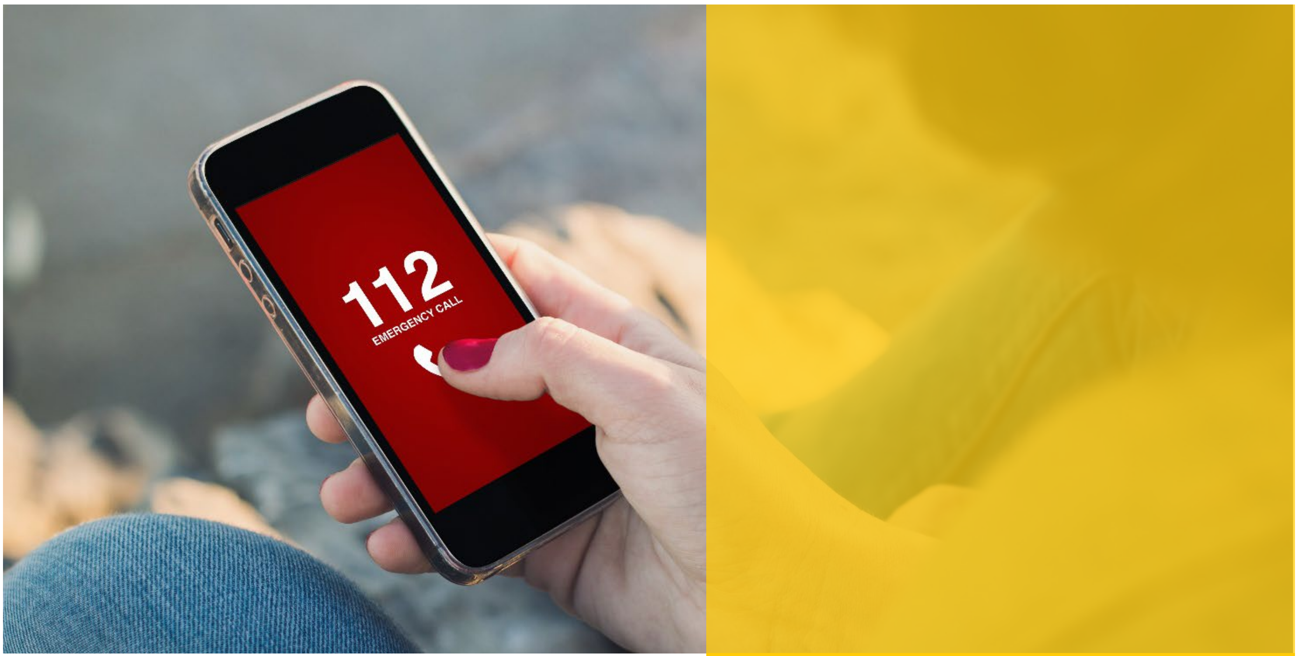
Fidel Liberal, UPV/EHU

René Lanz, Eviden

EENA
European Emergency Number Association
EENA

Avenue de la Toison d'Or 79, Brussels, Belgium
T: +32/2.534.97.89
E-mail: info@eena.org

Contents



EXECUTIVE SUMMARY

Emergency response teams now rely on advanced broadband networks, moving beyond narrowband voice and messaging to support IP-based multimedia for push-to-talk, video, and data sharing. NG112/911/999 and Mission Critical Communications (MCX) are becoming integrated, aiming to improve situational awareness, response times, and secure data sharing.

Currently, standards for emergency call handling and responder communications are evolving separately, but future interoperability is essential. This document focuses on the responder aspect of MCX, exploring its standards, infrastructure, and synergies with NG112, while highlighting the benefits of modern LTE/5G networks for emergency communications.

The purpose of this document is to:

- Provide an overview of MCX standards and certification
- Highlight the role of MCX in public safety operations
- Examine infrastructure and technology interoperability
- Present case studies and national initiatives
- Provide recommendations for future development and adoption

1. Definitions

Acronym	Desctription	Links
	ORGANIZATIONS	
3GPP	Third Generation Partnership Project	Link
ETSI	European Telecommunications Standards Institute	
ETSI EMTEL	ETSI Technical Committee Emergency Communications	Link
ETSI MSG	ETSI Technical Committee Mobile Standards Group	Link
ETSI TCCE	ETSI Technical Committee TETRA and Critical Communications Evolution	Link
MCCG	Mission Critical Communication Expert Group from DG Home	
TCCA	Tetra and Critical Communications Association	
CCBG	Critical Communications Broadband Group from TCCA	
GCF	Global Certification Forum	Link
MCS-WS	A joint Mission Critical Services Work Stream open to all stakeholders (Mission Critical Operators, Service Providers and Public Agencies, Device Manufacturers, Mission Critical client and server vendors and Test industry)	Link
O-RAN	Open Radio Access Networks (OpenRAN) Alliance	Link
FirstNet Authority	First Responder Network Authority is an independent agency within the U.S. Department of Commerce's National Telecommunications and Information Administration	Link
NPSTC	National Public Safety Telecommunications Council is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership	Link
	TECHNOLOGY	
2G, 3G, 4G, 5G	2nd, 3rd, 4th and 5th generations of mobile network technology. Electronic communications on 4G and 5G networks rely exclusively on IP-based communications.	
Bandwidth	Bandwidth represents the range of frequencies used in communication. Based on the size of the frequency band, there are two classifications: **narrowband** and **broadband**. Narrowband signals cover only a small fraction of the frequency spectrum, whereas broadband signals occupy a fairly substantial portion.	
EUCCS	EU Critical Communication System within BroadEU.net	

LTE	Long Term Evolution (4th Generation or 4G)	
MC	Mission Critical. Quality or characteristic of a communication activity, application, service or device, that requires low setup and transfer latency, high availability and reliability, ability to handle large numbers of users and devices, strong security and priority and pre-emption handling. Mission Critical Applications are generic communication applications with mission critical characteristics, traditionally encompassing push-to-talk voice, real-time video and real-time data.	
MCBBE	Mission Critical Broadband Environment (BroadEU.net)	
MCC	Mission Critical Communications	
MCX	Mission Critical Voice, Video and Data services	
MCPTT	Mission Critical Push-To-Talk (voice). Standard that defines the requirements for push-to-talk over LTE to mirror the mission-critical voice communication services provided by land mobile radio systems.	
MCVideo	Mission Critical Video -> Real-time video.	
MCData	Mission Critical Data -> Real-time data	
MCOP	The Mission Critical Open Platform Project	Link
FRMCS	Future Railway Mobile Communication System that is based on Mission Critical Features	
RAN	Radio Access Networks	
	REGIONAL NETWORKS	
BroadEU.net	BroadEU.net is funded by the European Union's Internal Security Fund	Link
ESN	Emergency Services Network in the UK	Link
FirstNet	First Responder Network in the USA; communications network dedicated to emergency responders and the public safety community.	Link
POLYCOM	Switzerland's secure radio network	Link
RRF	*Réseau Radio du Futur* (French) // Radio Network of the Future (English)	

2. Introduction

When response teams are deployed in emergency and crisis situations, they need to communicate with each other and with the control rooms. The way they do so has been evolving continuously with new devices, new communication channels, new networks and new standards.

What some years ago was limited to voice and short-messaging based communications using narrowband networks, is today geared to broadband networks with full IP and multimedia communications for PTT, Video and Data.

Thus, Next Generation 112/911/999 (NG112/911/999) & Mission Critical Communications (MCX) are becoming inextricably linked as critical components of the evolving public safety landscape and share common goals in terms of enhancing situational awareness, improving response time & communications interoperability.

Some common goals include secure, crisis-resistant transmission of voice, data and images. These address evolving multimedia communication needs, recording needs, asset location needs and interagency cooperation. This applies even in cross-border activities and extreme situations affecting communications and is especially relevant when PSAP and Control Room operations are fully integrated.

Currently, emergency and crisis communications evolve in two separate streams of innovation and standardization. A true combination of these two streams has yet to occur:

- The "requester" side, where people contact PSAPs for help, is covered by NG112/NG911/NG999 standards for the ESInet and NGCS and IP based communications (including eCall, PEMEA and more)
- The "responder" side, where emergency response teams in the field communicate, is governed by 3GPP and other standards for broadband networks and communications.

At the 2024 EENA Conference there was a session on "*NG112 & MCX: A Convergence of Innovation for Public Safety*". The session included two interesting presentations on GIS interoperability and mission critical communications in roaming environments.

Moreover, in EENA's 2023 document on *Data Sharing*, broadband communications requirements for data sharing between the different stakeholders were introduced which may or may not be in the same country or in the same network.

The purpose of the present document is to provide a perspective on the "responder" side of things and the synergies between the NG112/911/999 world and the MCX world.
The document is structured in 4 sections:

1. Ongoing MCX standardization and certification
2. Information on the pan-European initiative BroadEU.net
3. A focus on the infrastructure of MCX compared to NG112/911/999
4. National approach examples
5. Recommendations

Differences from currently deployed narrowband technologies like Tetra, Tetrapol to broadband deployments, using LTE/5G frequencies:

- Tetra 1 (original configuration) achieves data rates of about 28.8 kBit/s
- Tetra 2 (original configuration) achieves data rates between 134 kBit/s up to 500 kBit/s (4 timeslots) – Tetra 2 is actually a wide-band system.
- Tetrapol: 4.8 kBit/s per channel
- For 4G/5G, depending on the available bandwidth, experts speak of the following gross data rates - If you want to encrypt your traffic, the BW will be reduced. Keep in mind that you might have to share the available bandwidth with multiple participants in the network.
    - Link to calculate bandwiths: *https://www.cellmapper.net/4G-speed*
    - 3 MHz Bandwidth: Downlink: 22.5 Mbit/s, Uplink 7.5 Mbit/s) [Normally UL/DL ratio can be changed if needed]
    - 5 MHz Bandwidth: Downlink: 37.5 Mbit/s, Uplink 12.5 Mbit/s) [Normally UL/DL ratio can be changed if needed]

In summary:

- Much more bandwidth is available, and as you have an IP network with 4G/5G, different applications can be run.
- Additionally, 4G/5G networks follow the 3GPP specifications, which means less vendor lock-in than with Tetrapol (only one vendor) or Tetra (different dialects from different vendors, not perfectly compatible).
- Also, easier interoperability with existing MNO networks, as they also use the 4G/5G techno, ie. for roaming, handover scenarios.
- And Hybrid deployment models can be used (government network using multiple MNO coverage + dedicated base stations on another band), are possible.

3. MCX standardization and certification

MCX standardization is led by 3GPP and there is also a workstream in ETSI's Technical Committee TETRA and Critical Communications Evolution (TCCE).

Additionally, the O-RAN Alliance defines OpenRAN (with ETSI adopting their specifications), and GCF together with TCCA provide a certification for Broadband Mission Critical Services.

3GPP standards

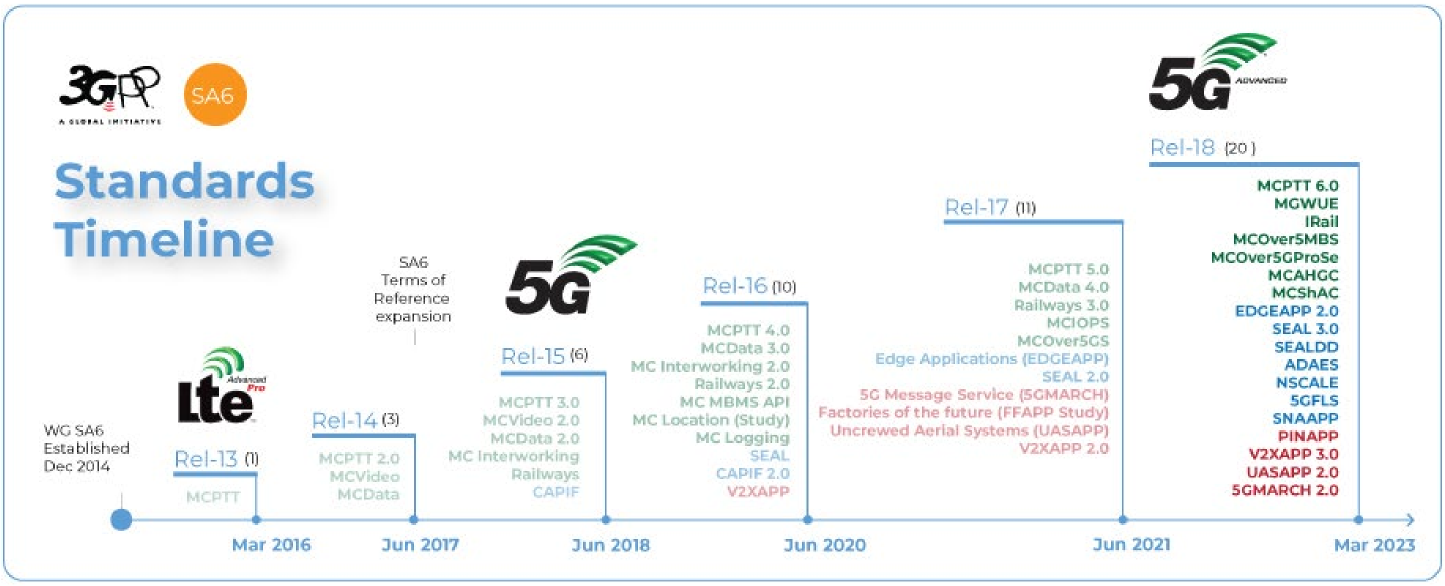
Source: https://www.3gpp.org/technologies/sa6-cc-apps

3GPP deals with a number of 3G/4G/5G services dedicated to public safety.

Mission Critical (MC) standards development in 3GPP started in 2015 in Release 13 following a major initiative from the public safety industry to create global standards with the collaboration of various government organisations, vendors and users from around the world. 3GPP has also produced standards for eCall, for instance.

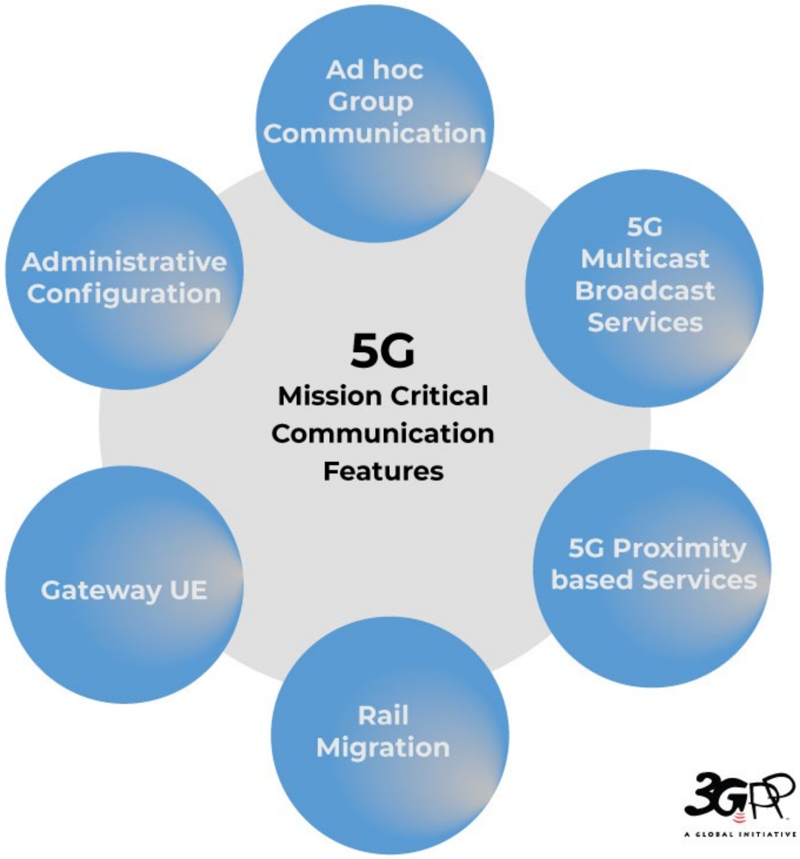
The diagram below depicts the evolution of 3GPP standards with its 3 core focuses:

- Mission Critical Services
- 5G Service Frameworks
- Vertical Application Enablers



The 3GPP SA WG6 is a dedicated group for Critical Communications applications and is responsible for the definition, evolution and maintenance of technical specification(s) for application layer functional elements and interfaces supporting critical communications (e.g. MCPTT and Mission Critical Video).

In Release 18, some of the key new features developed include:



- MC gateway UE, that enables MC service access for a MC service user residing on non-3GPP capable devices and for devices which cannot host MC service clients
- Ad hoc group communication, that allows an MC user to select other users and setup group communication on the fly across one or more MC systems
- MC services using 5G MBS supports both Multicast and Broadcast modes to provide efficient downlink delivery of user traffic in group communication
- 5G ProSe UE-to-network relay leverages newly designed radio and core network for providing MC service UE, connectivity and relaying of MC traffic to remote MC service UE(s), using 5G ProSe Layer-2 and Layer-3 UE-to-network relaying techniques
- Enhancements to the Railways functionality (applicable also for Mission Critical verticals) e.g. location management across MC systems, migration during ongoing communications.
- SA6 also completed a study (TR 23.700-38) for sharing of the administrative configuration between interconnected MC Service systems of MCPTT, for which the normative specification is expected in Release 19.

ETSI standards and plugtests

ETSI's work is well known within the EENA community, but it may not be as known in the field operations side of things.
We can highlight two ETSI Technical Committees dealing with public safety & emergency communications that are relevant for this document:

1. TC EMTEL (ETSI Technical Committee Emergency Communications) -> focusing on the "requestor" side of things.
    i. *6th NG112 Emergency Communications with NG eCall Plugtests* (30 September-4 October 2024)
    ii. Recent: *PEMEA Plugtests 2024* (12-16 February 2024)
2. TC TCCE (ETSI Technical Committee TETRA and Critical Communications Evolution) -> Focusing on the "responder" side of things. One of the ETSI Plugtests programmes is about MCX, with a definition of scenarios for Mission Critical Services, although the main focus is in the Railways domain as the Future Railway Mobile Communication System (FRMCS) is based on Mission Critical Features.
    i. Past: *8th MCX Plugtests* (9-13 October 2023). *ETSI TS 103 564* is about Plugtests scenarios for Mission Critical Services
    ii. Past: *4th FRMCS Plugtests* (1-5 July 2024) based on the same ETSI TS 103 564 joint technical specification.
3. TC MSG (ETSI Technical Committee Mobile Standards Group) -> Focusing on providing the regulatory standards needed to support the deployment of GSM, UMTS™ and LTE™ networks in Europe. They are working closely with O-RAN to adopt their specifications as ETSI Technical Specifications.

O-RAN Alliance

Source: *https://www.o-ran.org/*
O-RAN ALLIANCE was founded in February 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange. Since then, O-RAN ALLIANCE has become a world-wide community of mobile network operators, vendors, and research & academic institutions operating in the Radio Access Network (RAN) industry.

- O-RAN ALLIANCE's mission is to re-shape the RAN industry towards more intelligent, open, virtualized and fully interoperable mobile networks.
- O-RAN specifications enable a more competitive and vibrant RAN supplier ecosystem with faster innovation to improve user experience.
- O-RAN ALLIANCE operates in compliance with WTO principles for the development of international standards, guides and recommendations: transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and addressing the concerns of developing countries.

In 2022, ETSI and O-RAN announced that ETSI adopted the first O-RAN specification as ETSI TS 103 859, namely '*O-RAN Fronthaul Control, User and Synchronization Plane Specification v7.02*' (*link*)

O-RAN Global PlugFests are periodic events organized and co-sponsored by O-RAN ALLIANCE to enable efficient progress of the O-RAN ecosystem through well-organized testing and integration. Vendors and providers come together to test, evaluate and verify their products and solutions.

New certification for Broadband Mission Critical Services

Source: *https://mcsws.globalcertificationforum.org/*

GCF and TCCA develop and maintain a certification scheme for Mission Critical Services, focused on 3GPP MCS services, frequency bands and functionalities and priorities required by the mission critical industry.

- GCF is a non-profit, global membership driven organisation offering mobile and IoT certification programmes based on conformity to agreed standards.
- A joint Mission Critical Services Work Stream (MCS-WS) is actively maintaining this scheme, open to all stakeholders (Mission Critical Operators, Service Providers and Public Agencies, Device Manufacturers, Mission Critical client and server vendors and Test industry).

In June 2024, GCF announced the launch of a certification program for Broadband Mission Critical Services – in collaboration with TCCA (*link*), therefore adding 3GPP-based Mission Critical Services (MCS) to its certification programme, also referred to as MCX. That initial launch included MCPTT (voice) Release 14 clients and UE certification (associated with GCF Work Item WI-288). Other MCX services like MCData and MCVideo and new 3GPP releases are already considered in GCF plans for MCX clients and UEs certification. The certification of MCX servers (both in the server to client and server-to-server interfaces) is also already in consideration.

4. A pan-European initiative – BroadEU.net

A revised call for tender was published on the 23rd of August 2024, with a submission date for questions on 26 August 2024, and a submission date for the Call for Tender on 20 September 2024.

Source: *https://ted.europa.eu/en/notice/-/detail/505872-2024*

Source: *https://broadeu.net/*

BroadEU.Net is a partnership of Ministries, or their delegated representative agencies, in 16 EU and Schengen member states, plus an Operational Procedures Team of experienced responders. The European Commission is working with Member States to establish the EU Critical Communication System (EUCCS) to connect communication networks of all public law-enforcement, civil protection and safety responders in Europe by 2030 to allow for seamless critical communication and operational mobility across the Schengen area.

The BroadEU.net programme will work towards EUCCS to explore the needs of operational safety and security responders across Europe and test standardised technical solutions to realise Operational Mobility: the ability for responders to carry out their operations with mobile communications wherever they are, whenever they need to, and in cooperation with whomever they are tasked to cooperate.

BroadEU.Net builds upon the success of the project *BroadWay* which concluded in 2022.
BroadEU.Net explores both technical and operational matters. To build the understanding of governance, policy and legislation needed to support EUCCS, the European Commission (DG Home) recently initiated the Mission Critical Expert Group (MCCG), involving experts from all 31 EU and Schengen member states.

BroadEU.net Stage 2 prepares the ground for deployment and operational use of the EUCCS. Two main activities are planned:

- Mission Critical testbed deployment and technical testing: to build confidence in the technical maturity of 3GPP mission critical services.
- Operational Procedures: development and trial of new and amended operational procedures to support cross-border and pan-European police and civil protection response operations that will be enabled by EUCCS.

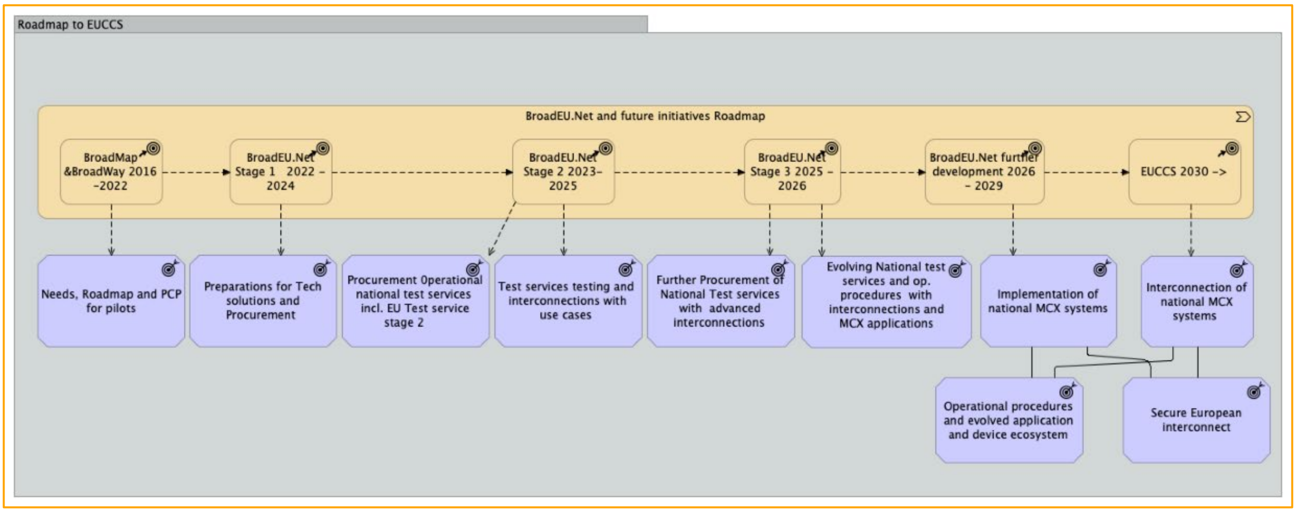
MCX Testbeds will be procured, deployed and hosted nationally. They will be interconnected across countries to test, scale up and trial the technical feasibility of deployed 3GPP Mission Critical (MCX) services. This leverages the valuable outcomes of the BroadWay project which has already proven the technical feasibility in 3 large scale trials.

In BroadEU.Net, the system will be continually live and MCX services will be deployed initially in 5-7 countries. Further stages will see an expansion to include additional countries. A team representing responder organisations will use the MCX technology in real life scenarios to trial new operational procedures. BroadEU.net will engage with the entire eco-system spanning EU and Schengen Member States, Industry and the Research community.

- Operational challenge: The BroadWay project demonstrated that technical solutions are available to achieve cross-connected MCX services and the ability to communicate between different systems operated by different administrative domains. In BroadEU.Net, emphasis is on operational need for MCX server-to-server interconnection services. Operational need is the driving force which will determine the scope of MCX services and the need for technical and operational interconnection.
- Technical challenge: The technical challenge involves systematically testing the MCX server-to-server interconnection. To do this, national MCX testbeds must be established. These testbeds will include MCX services, MC testing apps, MC operational procedure apps, and mobile devices. Once set up, the national testbeds will be interconnected to address the "Operational Challenge." The testbeds procured in BroadEU.Net Stage 2 will also be used in Stage 3 and beyond, with the goal of realizing EUCCS in the coming years.

Roadmap

The following roadmap to EUCCS is a general view for BroadEU.net project tasks and goals obtained from the following *link*.

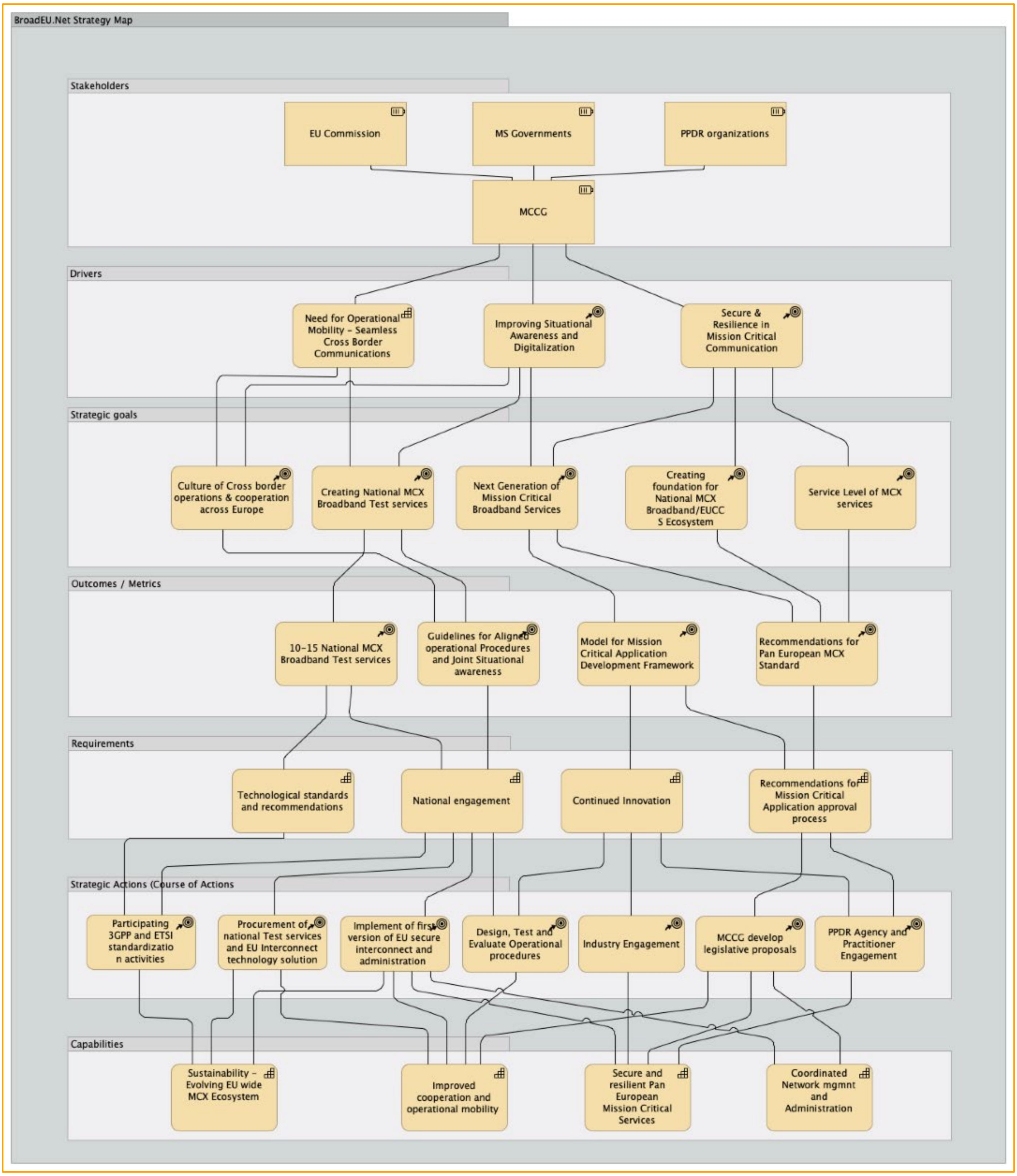


Strategy

This Strategy Map is a tool for steering the work for BroadEU.Net project, obtained from the following *link*. The map consists of views for:

1. Stakeholders
2. Drivers for the BroadEU.Net project
3. Strategic goals
4. Outcomes/Metrics of the process
5. Requirements to achieve goals

6. Strategic actions
7. Capabilities created to European Public and Safety actors Also, dependencies and connections with the strategic elements are shown in each view



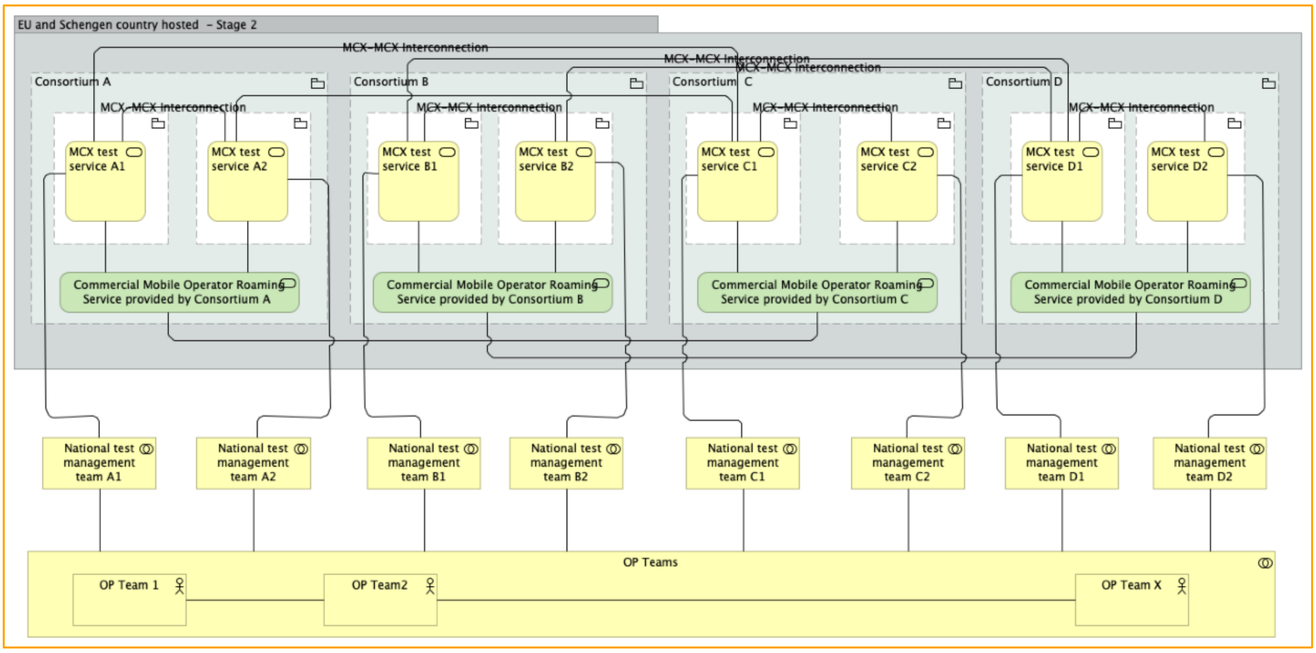
Architecture

Source: https://arch.broadeu.net/

A first view on the BroadEU.Net architecture was available after the Open Market Consultation questionnaire, and a limited set of views were provided to illustrate initial context, with further detail being added in the course of the BroadEU.Net programme to take account of technical views, to include the wider strategic context and to support development of Operational Procedures.

This architecture is intended to provide a holistic model to support the development of solutions, which can be used in real operations in future, when technical and operational maturity is achieved.

A high-level reference architecture for procurement has been proposed in version 2 of the BroadEU.net architecture. The diagram below illustrates the MCX-to-MCX interconnections within the MCX Test Services.



Roaming

The Broadway project produced significant results focused on crisis situations and cross-border scenarios. An example presented by GSMA at the EENA Conference 2024, during the session "NG112 & MCX: A Convergence of Innovation for Public Safety". The presentation can be downloaded from the following link.

The Joint Mission Critical Task Force (MCTF), established in July 2023, worked on identifying the requirements and technical aspects of implementing MCX services in roaming environments. They produced a white paper providing guidelines for implementation, with their primary focus (TF PH1) on mission critical services affecting 4G and 5G NSA networks architecture.
The presentation covered use cases, such as critical events like wildfires and police pursuits and data automation in the railways sector. Key technical aspects mentioned in the presentation included.

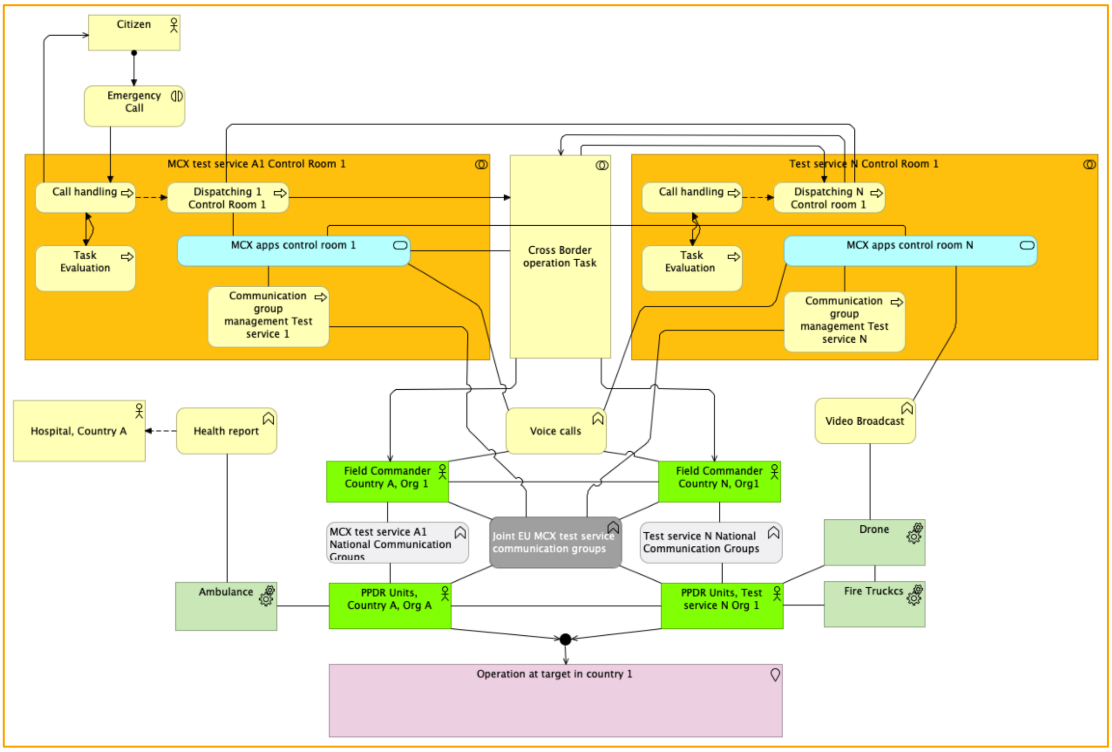
Key technical aspects mentioned in the presentation included:

- Type of home / visited networks (4G standalone, 4G Hybrid, 5G NSA...)
- Type of QoS (Latency, Packet Error Rate, Packet Delay, Throughput...)
- Type of traffic (MCPTT, MCdata, MCvideo, Voice/Volte, SMS, ...)
- Type of users and required connection (PSBN roamers, MNO roamers, UE devices)

The presentation also provided details on the major topics to be technically evaluated:

- Services and Quality Parameters
- Access Priority
- Seamless Mobility
- Roaming Agreements
- Steering of Roaming
- Wholesale
- Billing
- Legal and Regulatory

A cross-border operational example is also available in the BroadEU.net architecture page in the following *link*.

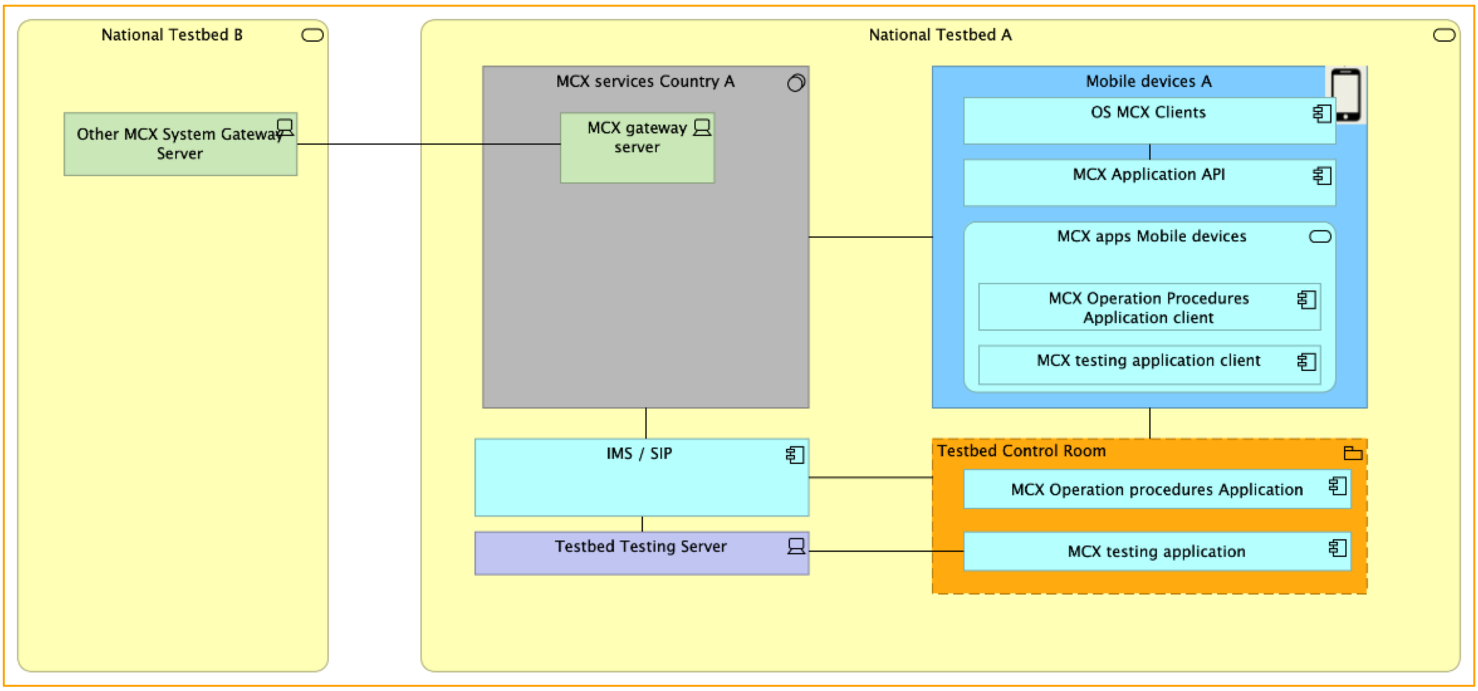


5. Overview of infrastructure: MCX vs NG112

When discussing end-to-end critical communication provisions, several key areas must be addressed:

1. Infrastructure
2. Devices
3. Applications
4. Integrations
5. Maintenance

Focusing on infrastructure, one critical consideration is the potential synergies between the MCX ecosystem and the NG112/911/999 ecosystem.
In the context of the MCX ecosystem, below, we examine the components proposed for national testbed procurement within the BroadEU.net architecture:



We then examine the NG112/911/999 ecosystem by considering the ESInet & Core Elements architecture as described in ETSI TS 103 479 (*link*):

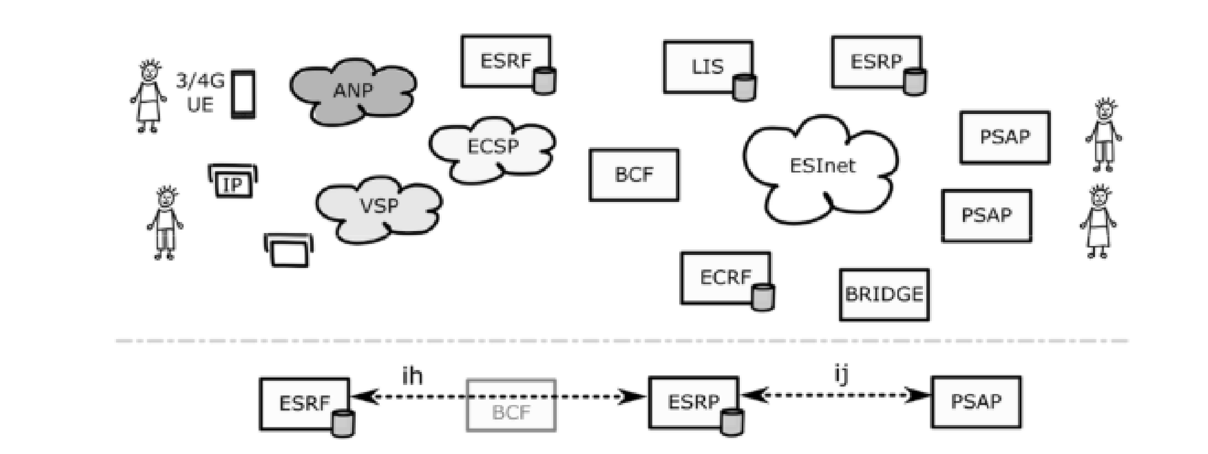
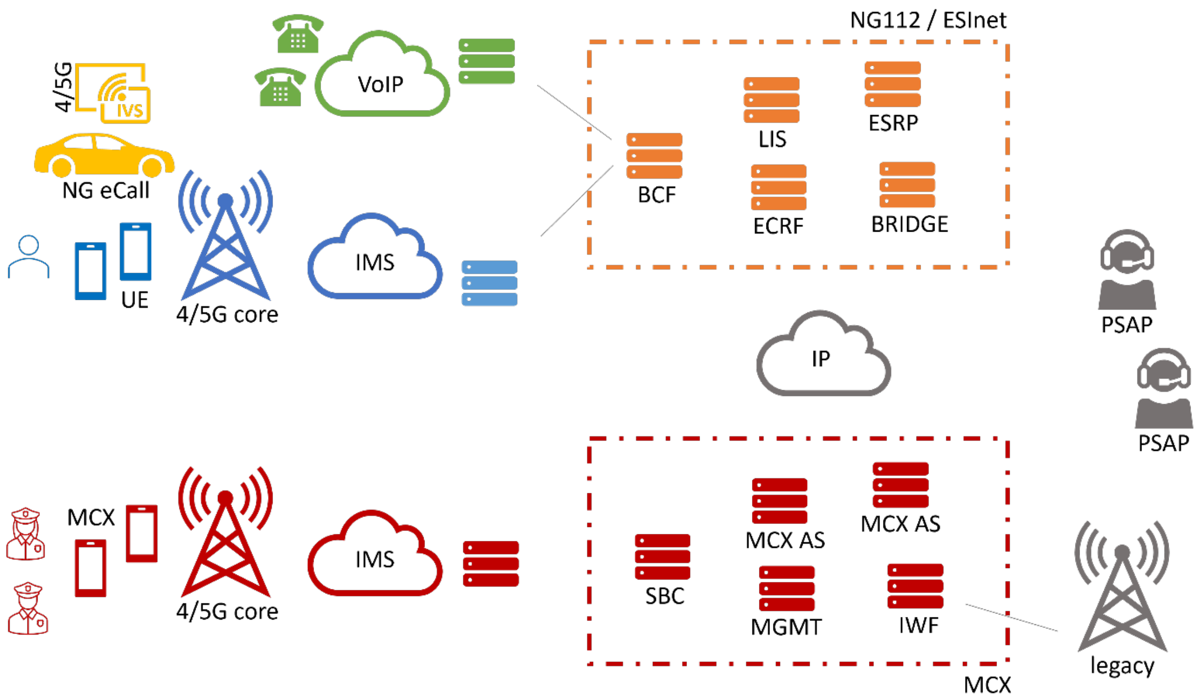


Figure 1: High level functional architecture

Both NG112 and MCX aim to improve public safety communication systems. NG112 modernizes emergency services by integrating new communication technologies, while MCX provides reliable communication for public safety and emergency responders.



Both systems use IP-based technologies to enhance communication capabilities, including support for multimedia communications such as voice, real-time text, video, and data. They emphasize interoperability, with NG112 ensuring international interoperability for emergency services, facilitating global standards, and MCX focusing on interoperability among public safety agencies and communication networks.

NG112 and MCX can share a common IP network infrastructure due to their reliance on IP-based technologies for communication. By leveraging a common IP backbone, these systems can handle various types of communication traffic, including voice, text, video, and data. NG112 relies on the Emergency Services IP Network (ESInet) to route emergency calls and data. ESInet is designed to be a highly resilient and secure network that supports multimedia communications.

MCX services can also utilize ESInet for mission-critical communications, ensuring that all emergency-related data is transmitted over a robust and reliable network. A common IP network infrastructure can implement Quality of Service (QoS) mechanisms to prioritize mission-critical traffic. This ensures that emergency communications, whether from NG112 or MCX, receive the highest priority, reducing latency and improving reliability. QoS settings can be configured to prioritize voice and video calls, real-time text, and critical data transmissions.

Using a shared IP network infrastructure facilitates interoperability between NG112 and MCX systems. This integration allows for seamless communication and data sharing between emergency call centres and first responders. For example, data collected through NG112, such as caller location and other incident data, can be instantly shared with MCX-enabled devices used by first responders, enhancing situational awareness and response coordination. A common IP network infrastructure provides scalability and flexibility, allowing for the addition of new services and technologies as they become available.

Sharing a common IP network infrastructure reduces the need for separate networks, leading to cost savings in terms of deployment, maintenance, and operation. This consolidated approach allows for more efficient use of resources and budget. A unified network infrastructure enhances coordination between emergency services and public safety agencies. Managing a single network infrastructure simplifies network administration and monitoring.

NG112 primarily focuses on emergency call handling and routing, integrating modern communication methods like text and video calls into emergency services. This allows emergency call centres to receive, and process calls more efficiently, providing better service to the public. In contrast, MCX encompasses a broader range of mission-critical communication services, including Mission Critical Push-to-Talk (MCPTT), Mission Critical Data (MCData), and Mission Critical Video (MCVideo). These services support various public safety operations beyond emergency call handling, such as real-time coordination during incidents and sharing critical information among first responders.

NG112 involves upgrading emergency service infrastructure to support accessible emergency communications. This includes deploying an Emergency Services IP Networks (ESInet) and ensuring compatibility with various communication devices and platforms. MCX, on the other hand, is typically implemented over dedicated or hybrid public safety networks, such as LTE and 5G, to ensure high reliability and low latency for mission-critical communications. These networks are designed to provide robust and secure communication channels for public safety agencies, ensuring that they can communicate effectively during emergencies.

NG112 enhances the efficiency and accessibility of PSAPs by supporting features like location-based call routing, and conveyance of dispatchable locations, which allows emergency services to quickly determine the location of a caller and dispatch help more efficiently.

MCX supports a wide range of public safety operations. For example, Mission Critical Push-to-Talk (MCPTT) allows first responders to communicate instantly with each other, like traditional radio systems but with enhanced capabilities. Mission Critical Data (MCData) enables the sharing of critical information, such as maps and incident reports, while Mission Critical Video (MCVideo) allows for real-time video streaming, providing situational awareness during incidents. The MCX Common Service Core (CSC) components enable centralised authorization, authentication, configuration and group management mechanisms. Such core ecosystem, together with Location management capabilities and Inter working (IWF) and inter-MCX service enablers support a multi-technology (i.e. TETRA/Tetrapol/PMR/P25/MCX) and multi-agency coordination.

In summary, NG112 and MCX can share a common IP network infrastructure by leveraging core network components, ESInet, QoS mechanisms, and interoperability features. This shared infrastructure offers benefits, such as cost efficiency, enhanced coordination, improved reliability, and streamlined management, leading to more effective and resilient emergency communication systems. While both NG112 and MCX aim to enhance emergency communications, they serve different purposes and have distinct features. NG112 focuses on modernizing emergency call handling, integrating new communication methods to improve the efficiency and accessibility of emergency services. In contrast, MCX provides a comprehensive suite of communication services for public safety operations, supporting real-time coordination and information sharing among first responders. By leveraging IP-based technologies and emphasizing interoperability, both systems contribute to creating more effective and resilient emergency communication networks.

6. National approach examples

Given the national or regional competences of public safety operations in different countries, and the absence of specific regulations governing intra and inter-agency communications and information exchange, various approaches can be observed.

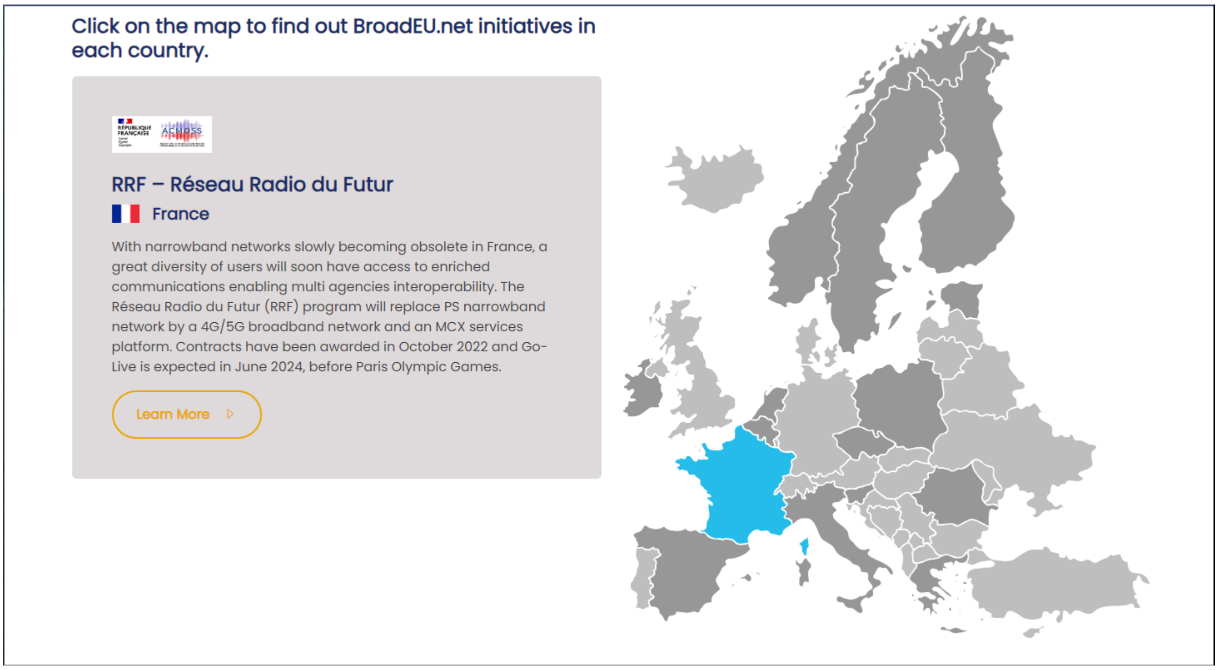
Across Europe, voice-centric communications between field responders control rooms are primarily conducted using traditional Radio devices (PMR, TETRA, TETRAPOL, Marine, Air Traffic, etc.) In some regions, data exchange is facilitated by the open EDXL framework by OASIS. For example, in Spain's Extremadura region, incident data is shared between the regional 112 PSAP and field responders via a mobile app.

However, new devices and applications compatible with MCC standards, for MCVideo, MCData are becoming available.

The shift from narrowband to broadband communications – from PMR, TETRA, TETRAPOL, P25 to 4G LTE and 5G, is becoming increasingly prevalent, both at national and tactical levels, to support services like MCPTT, MCData and MCVideo. These technologies offer higher throughput, additional services, and lower latency.

Investment in dedicated RANs could be reduced by leveraging existing MNO infrastructure, with the option to deploy dedicated/private networks to enhance resilience, autonomy and meet specific needs. In light of current geopolitical tensions, the need for resilient and autonomous systems is becoming increasingly urgent.

The following map of BroadEU.net provides an overview of national initiatives in several countries in Europe (the example shows France): *https://broadeu.net/map/*



France – RRF

The Réseau Radio du Futur (RRF) program will replace PS narrowband network by a 4G/5G broadband network and an MCX services platform (contracts were awarded in October 2022 and Go-Live was expected during 2024).

Link to video of RRF experimentation during the Rugby World Cup 2023.

Extract and shortened version
from: https://www.interieur.gouv.fr/archives/actualites/communiques-de-presse/lancement-du-projet-reseau-radio-du-futur-rrf-reseau-tres-haut
https://www.acmoss.fr/

The Future Radio Network (*Réseau Radio du Futur*, RRF) is the French State's response to modernize the communication of security and relief actors. Today, police officers, gendarmes, firefighters, SAMU doctors use radio equipment designed in the early 1990s, specific to each force, which does not allow the transmission of large amounts of data or images in real time from the field.

With RRF, France will equip itself with a very high-speed communication network (4G then 5G) common to all the actors of security and rescue, allowing them to communicate instantaneously with each other by benefiting from new functionalities: video calls, live position sharing, sending electrocardiograms, etc. RRF considers more than 300’000 users participating in the security domain and allows the field officers to be connected to the command rooms. Through its very robust infrastructure, the RRF will provide its users with a highly resilient network, ensuring continuity and security of communications throughout the country.

Beyond its operational challenges of protecting the population, RRF is a real industrial project that makes France a central player in the strategic field of critical radio communications on a global scale. With an investment of more than EUR 700 million from the Ministry of the Interior, it is a unique opportunity to consolidate the French industrial sector and to reap the benefits in terms of jobs - as well as for exports - with the structuring of a credible supply vis-à-vis other global players.

Timeline:

- With the notification of the market for the RRF implementation, the Ministry of the Interior started the construction of the future network in September 2022.
- The construction and testing of a first version of the RRF would run over a period of 19 months, making it possible to secure the technical robustness of the solution and its appropriation by future users.
- It will use the commercial infrastructures of the Orange and Bouygues Telecom networks. The system itself will be built mainly by a consortium of Airbus and Capgemini, and the information system by Atos/Eviden.
- From 2024 onwards, RRF is to become the backbone of the operational communications of the security, rescue and crisis management actors.

Switzerland – POLYCOM

Polycom, rolled out by Siemens/Atos/Eviden, is the nation-wide secure radio network of rescue and security authorities and organisations (BORS) used by about 55,000 users daily. It enables Tetrapol radio communication within and between the various organisations Border Guard, police, fire service, ambulance, civil protection organisation and supportive military units. Today, all Tetrapol users of the Confederation, cantons and communes are able to transmit both voice and data messages through a uniform infrastructure. The secure network was established step-by-step with modular networks under the direction of the Federal Office for Civil Protection (FOCP). The FOCP's training centre in Schwarzenburg offers courses necessary for operating the network and training the end-users.

The rollout of the first Polycom base stations started in the year 2000 and was concluded in 2015. A large portion of the components used in the Polycom system has been in operation for decades and needed to be renewed due to lifecycle considerations. In 2016, FOCP initiated the Polycom 2030 project to renew 782 base stations and all other Tetrapol infrastructure from TDM to IP to ensure Polycom operation at least until 2030 and to provide for sustained value of the entire system.
Atos/Eviden will conclude the migration in 2025, until then Tetrapol and TDM/IP systems will be operated in parallel.

Extract and shortened version from: https://www.babs.admin.ch/de/msk

- Switzerland currently lacks a standardized system that ensures mobile broadband security communication for the Confederation, cantons and third parties in all situations. With the timely introduction of a future-oriented, mobile, broadband security communication system (MSK), communication between the authorities and organizations for rescue and security (BORS) should continue to be reliably guaranteed.
- For the secure and crisis-resistant transmission of voice, data and images and to close the identified gaps from Polycom, MSK shall be set up in 2026 and be introduced from 2030
- MSK will be based on the existing infrastructures of Polycom and commercial mobile communications providers, expanding them with crisis-resistant elements such as an independent emergency power supply and thus enabling seamless data communication.
- MSK thus complements the national secure data network (SDVN+) with secure mobile data communication.

Timeline

- In June 2024, the Federal Council opened a consultation on the replacement of Polycom by a national MSK with the financial, personnel, organizational and time-related implications. The consultation, coordinated by FOCP, offers all stakeholders a platform to help shape this forward-looking initiative. The consultation will run until October 24, 2024.
- Following the consultation process, FOCP will evaluate the comments received and submit a draft dispatch to the Federal Council.
- According to the current timetable and subject to government decisions, Parliament will be able to address the issue in 2025.
- This should allow the first stages of the project to be implemented in 2026.
- Planned total costs: around CHF 3 billion, including investments of around CHF 1.1 billion

UK – ESN

While producing this document, the UK Home Office was in a tendering process for a number of ESN elements so publicly available material was going to be very limited. Also, there may be some impact on timelines from the recent General Election and the changes it brought.

Extract and shortened version from: *https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network*

The Home Office is leading a cross-government programme to deliver the new Emergency Services Network (ESN) critical communications system. This will replace the current Airwave service used by the emergency services in Great Britain (England, Wales and Scotland) and transform how they operate.

ESN will enable fast, safe and secure voice, video and data across the 4G network and give first responders immediate access to life-saving data, images and information in live situations and emergencies on the frontline.

Users for ESN include the fire and rescue, police and ambulance services, as well as other users stretching from local authorities and utility services to first responders like inshore rescue. There are more than 300,000 frontline emergency service users who will depend on ESN; using handheld devices or operating equipment in 45,000 vehicles, over 90 aircraft and more than 100 control rooms.

ESN will deliver:

- secure and resilient mission critical communications the emergency services and other first responder communities can trust to keep them safe
- a modern voice and data platform which will enable the emergency services to improve front-line operations
- a common platform to enable emergency services to work more closely together for data sharing in emergencies

USA – FirstNet

Extract and shortened version from: *https://www.firstnet.gov/network*

The First Responder Network Authority, or the FirstNet Authority, is an independent agency within the U.S. Department of Commerce's National Telecommunications and Information Administration (NTIA) that oversees FirstNet, the nation's communications network dedicated to emergency responders and the public safety community.

The FirstNet Authority also coordinates with public safety through the Public Safety Advisory Committee (PSAC), which provides guidance and subject matter expertise from a first responder perspective.

FirstNet was created to be a force-multiplier for first responders — to give public safety the 21st century communication tools they need to help save lives and keep our communities safe.
To realize that vision, the FirstNet Authority is directing the deployment of a high-speed network using public safety's Band 14 spectrum. Built on commercial standards, the FirstNet network is resilient, interoperable, and able to provide optimal levels of operational capability during emergencies.

The FirstNet network is helping connect first responders during major emergencies and at large events by providing a "fast lane" for their highly secure communications. FirstNet delivers specialized features to public safety that are not available on most commercial wireless networks today, such as priority access, pre-emption, more network capacity, and a resilient, hardened connection.
The network operates in all U.S. states, territories, and Washington, D.C., transforming emergency communications nationwide. FirstNet delivers the benefits of lower costs, consumer-driven economies of scale, and advanced communication capabilities to public safety personnel.

Nevertheless, there are examples in which FirstNet is being used as backup for NG911, as with the Tennessee Emergency Communications Board and AT&T (source: *link*):

"Tennessee has embarked upon a plan to fully back up every one of its 9-1-1 call centers with AT&T ESInet™ and FirstNet® – America's public safety network – to increase their reliability and resiliency. This is a major step forward for public safety as Tennessee leads the way to become the first state in the nation to implement full wireless backup through FirstNet, Built with AT&T to all 9-1-1 call centers statewide. Wireless backup means that even during the toughest strains and worst-case scenarios, network connectivity will be available so that every Tennessean can know that 9-1-1 telecommunicators will answer their call.

How does it work? If AT&T ESInet detects a disruption to the primary 9-1-1 call center connections, it will automatically re-route 9-1-1 calls over the FirstNet network, ensur ing they are answered."

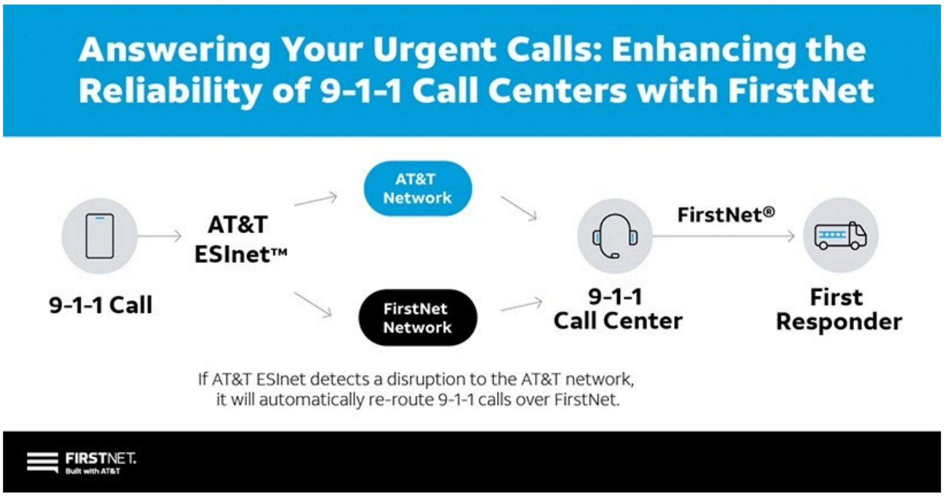


Figure 1: Source in link

Additional initiatives:

National Public Safety Telecommunications Council (*link*): NPSTC is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

NENA started a so-called STA-031.1 NENA Standard for Interconnecting Emergency Services IP Networks and Public Safety Broadband Networks.

7. Recommendations and closure

- Given current worldwide geopolitical tensions, the need of resilience and autonomy is paramount.
- Carefully plan the transition from narrowband to broadband and think about mutualising infrastructure shared with other "branches" of operations.
- Avoid vendor lock-in enhancing interoperability across vendors by requiring standards like 3GPP, OpenRAN.
- Consider reducing investments and effort to build up dedicated RAN by utilizing existing MNO coverage.
    - Dedicated PMR networks e.g. inB28 PPDR /B68 PPDR can be deployed additionally for resilience, autonomy, dedicated needs.
- Consider synergies with NG112/911/999 ecosystems for potential mutualisation of effort.