Deloitte.

Next Generation Mission Critical Networks

Global Telecom Engineering Excellence (gTEE)

1. Introduction

In a society moving towards digital, where access to data in almost real time is key to every single industry sector, Public Safety (PS) services are seen as laggers when it comes to take most of the technology available to enable agencies and emergency services to benefit the best information available. By relying in voice-centric technologies, Public Safety services cannot support themselves for instance on simple video-based use cases, which would leverage decision making processes with insightful information that could for example make a difference between life and death.

Land Mobile Radio (LMR) solutions are widely deployed around the world as Mission Critical Communications (MCC) Networks, enabling efficient voice communications with Push-to-Talk enabled services. Nevertheless, LMR architecture was designed as voice-centric at its core.

To address this data transfer limitation from LMR solutions, Public Safety entities have at their disposal 3GPP (LTE and 5G) based technologies capable of largely enhancing the scope of action of current LMR solutions. This happens by extending PS network capabilities with data-driven technologies and use cases far beyond the current voice-centric landscape provided by LMR.

In order to support with this MCC network modernization and targeting to move towards a solution capable of cope with heavy data-based use cases, Deloitte provides through this paper a detailed view of previous LMR solutions (TETRA and P25) and their limitations, as well as pinpointing the benefits from adopting 3GPP based solutions.

Two key underlying trends in public safety

Digital Leadership, embracing new technologies to enable a culture of collaboration and common mission and maximizing Data Usage within and across agencies to improve operational effectiveness

Next Generation Public Safety Organizations
Future organizations will embrace a multitude of digital technologies from field service augmentation, usage of drones and autonomous vehicles or other internet of things enabled solutions

Citizen Engagement
Exploring different channels and technologies to maximize the engagement and experience of citizens interacting with Public Safety related agencies

Data Sharing
Information sharing between public safety and other agencies providing mission critical services is key for the modernization of incident, investigation and critical situation management

Digital Government technology Platforms
Governments providing the right technical foundations will be key to leverage the shared services and enable their digital transformation from commodity towards value. Enhanced connectivity availability is one first step.

Situation Awareness
Situational awareness will leverage data, analytics and artificial intelligence to provide to multiple agencies and emergency services command a common operational view

Cybersecurity
Security and privacy are crucial in any digitalization transformation program, especially on Public Safety where attacks on related organizations will have a critical impact on the citizens well-being.

Figure 1: Gartner "Top Trends in Public Safety and Law Enforcement", Published: 10 January 2020

2. Why Mission Critical Communications are of utmost importance for Public Safety Agencies?

Citizen safety is extremely relevant for the national governments, therefore, the Public Safety Agents (PSA), such as firefighters and the police, should have a highly reliable and available network to enable both intra and inter agency communications to support their daily operations. Public Safety Networks aim to provide an appropriate communication support during PSA operations, allowing them to keep the order and the wellbeing of the general population, even during catastrophic situations (e.g., fires, earthquakes, terrorist attacks or criminal activity).

Following an increasing pattern of natural disasters and terrorist attacks (highlighted in the graphic below by the number of casualties), having a communication mechanism that supports and enhances PSA situational awareness is crucial, and serves as a facilitator for handling safety operations. Therefore, Mission Critical Communications (MCC) offering high availability and reliability, often granted by redundancies implemented on the MCC network, will end up saving lives. Additionally, being exclusive (or prioritized) to PSA, these networks will not be subject of congestion.

Having a communication mechanism that supports and enhances PSA situational awareness is crucial, and serves as a facilitator for handling safety operations

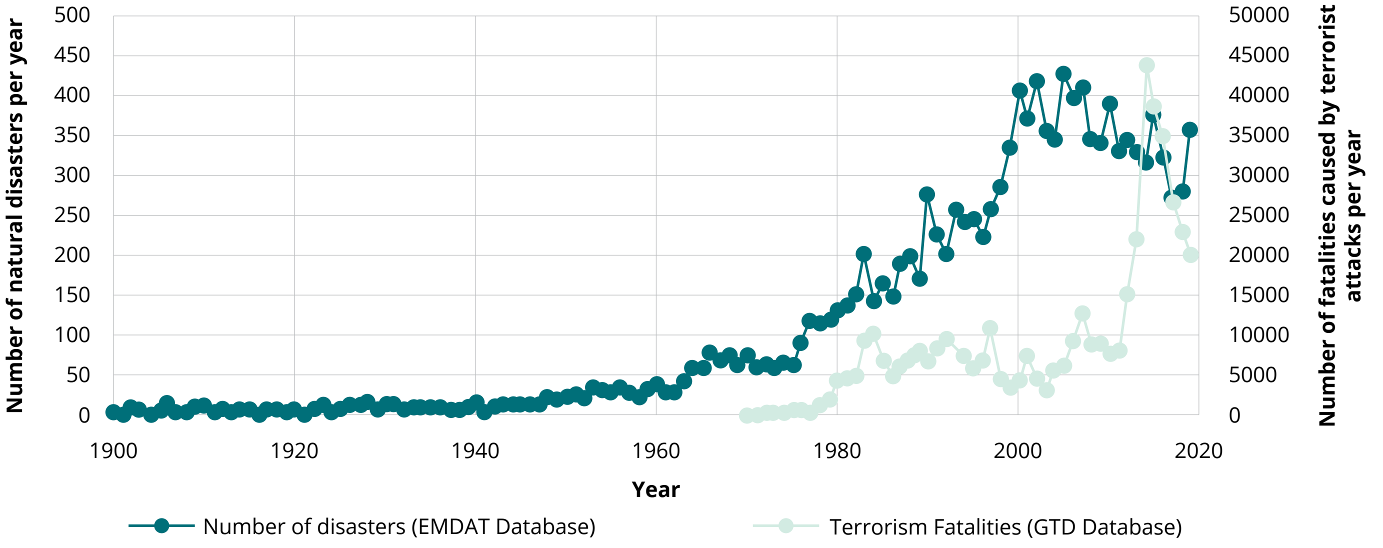


Figure 2: Number of natural disasters and fatalities caused by terrorist attacks. Source: [1]

Furthermore, MCC networks are expected to be more secure against cyberterrorism offering an added layer of security when facing more modern threats.

Considering the importance of human life and assets during critical moments, a proper and robust MCC network is imperative for Mission or Business Critical operations. With that in mind, a definition of MCC networks could be a "network that enables communication across several crisis scenarios, being available, reliable, resilient, and efficient across high demand scenarios in a way that supports PSA saving lives, assets, and minimizing environmental impacts caused by catastrophic scenarios". Narrowband technologies (such as LMR) have limited potential due to its design limitations (despite offering high levels of availability, reliability, resilience, and efficiency while handling high demand scenarios), narrowband technologies cannot address high volumes of traffic and therefore are not enablers of new use cases enabled by recently developed technologies (e.g., to this day to feed dispatch centers on how operations are evolving while fighting wild-fires it is often used helicopters, while with proper broadband technologies it would be possible to mitigate risks and use drones instead).

From those limitations the importance of moving to data centric broadband technologies which at this point are quite mature and could surpass narrowband technologies at several levels, instead of relying in voice-centric outdated and limited technologies, that will increase the situational awareness and efficiency of PSA operations.

Having LTE or 5G working as MCC networks requires them to comply with specific requirements, such as high available, reliable, efficient across high demand scenarios, resilient, and able to comply with the highest security standards , to minimize the probability of failure during catastrophic events and, consequently, to satisfy those requirements network hardening is often needed.

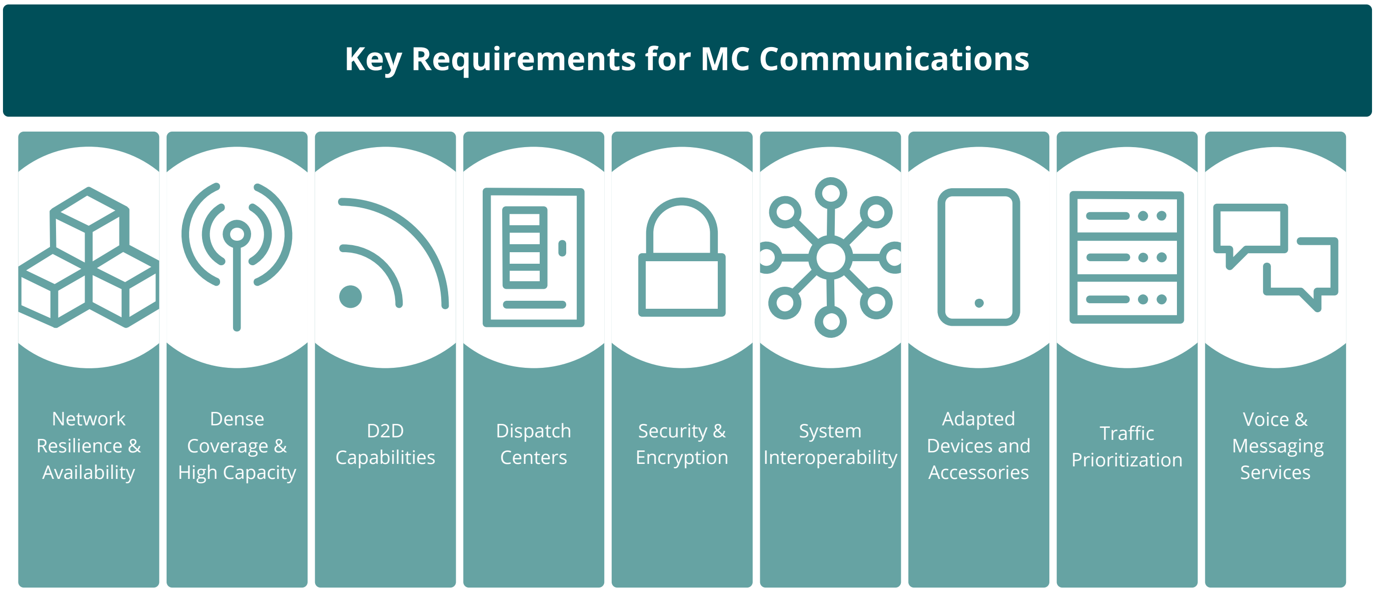

Key Requirements for MC Communications
Network Resilience & Availability
Dense Coverage & High Capacity
D2D Capabilities
Dispatch Centers
Security & Encryption
System Interoperability
Adapted Devices and Accessories
Traffic Prioritization
Voice & Messaging Services

Figure 3: Key requirements for Mission Critical Communications

Moving away from the already established voice-centric narrowband systems will require significant transformation on UE, Core, RAN, MCC applications and Dispatch Centers. Although it is understood that forementioned MCC applications and dispatch solutions play a major role in the end-to-end delivery of mission critical communication (please note that a detailed analysis for a transformation towards broadband in those areas goes beyond the scope of this document).

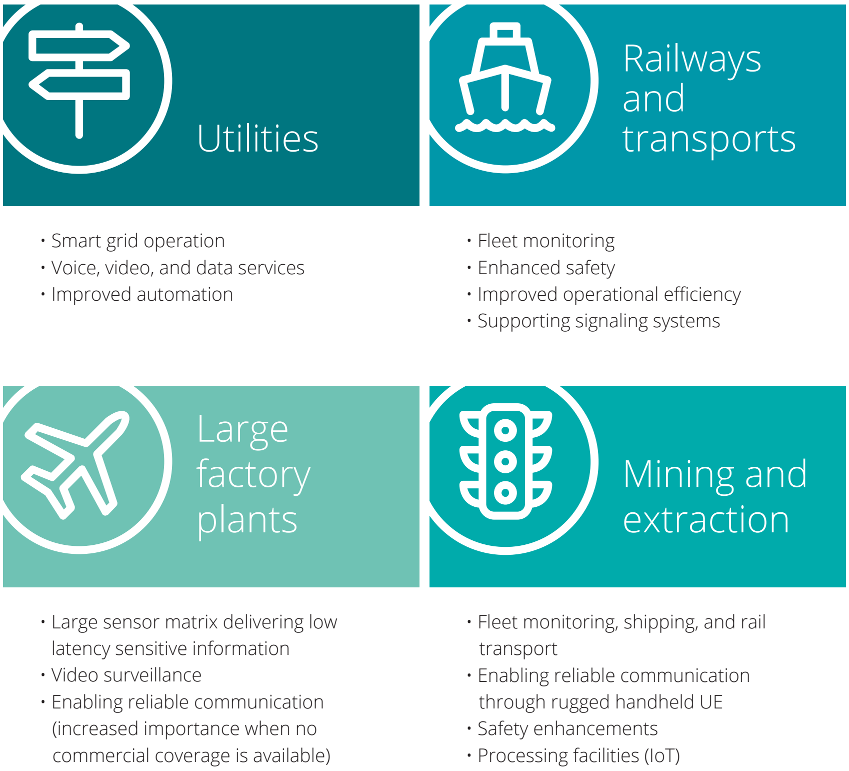
The goal of this Point of View is to provide a comprehensive overview of the cellular technologies that are currently implemented and to come up with a perspective on the migration to broadband technologies. The document supports the planning of a network that meets the needs of the Public Safety case, working efficiently and being cost-effective (without compromising security and safety), and building the foundation for next generation MCC applications.

A network that could enable communication across several crisis scenarios, being available, reliable, resilient, and efficient across high demand scenarios in a way that supports PSA saving lives, assets, and minimizing environmental impacts caused by catastrophic scenarios.

a) Mission Critical Networks for Industry

Some critical businesses or heavy industries require (and use) reliable, available, efficient, and robust communications and/or terminals. In these cases, Critical Communications across those businesses rely on the same specifications as MCC and, therefore, are designed as business critical communications (BCC). The failure of those communications can compromise human lives and the safety of citizens, assets, or the environment.

Like Public Safety, many industries still rely on Land Mobile Radio solutions, however there is a rising trend of implementing new use cases over Private LTE/5G networks or relying on 5G Network slices to do so:



Utilities

- Smart grid operation
- Voice, video, and data services
- Improved automation

Railways and transports

- Fleet monitoring
- Enhanced safety
- Improved operational efficiency
- Supporting signaling systems

Large factory plants

- Large sensor matrix delivering low latency sensitive information
- Video surveillance
- Enabling reliable communication (increased importance when no commercial coverage is available)

Mining and extraction

- Fleet monitoring, shipping, and rail transport
- Enabling reliable communication through rugged handheld UE
- Safety enhancements
- Processing facilities (IoT)

Figure 4: Industry verticals where MCC are being adopted to create efficiencies and enhance security

Source: [(2)]

Business Critical Communications are expected to **deliver highly reliable, available, secure and being enablers of data-centric use-cases.** A rising trend has been established in some sectors concerning the implementation of Private LTE/5G networks. According to IDC forecasts, private LTE/5G infrastructure revenues growth from $1.7 billion in 2021 to $8.3 billion by 2026, representing a CAGR of 35.7% over the 2022-2026 period.

The focus of this PoV is on Public Safety, therefore BCC trends will not be further detailed in this document. However, this type of communications can be seen as a Proof of Concept (PoC) of smaller MCC networks already operating PS-like services on different industries.

3. Narrowband Systems - Characteristics and Limitations

Terrestrial Trunked Radio (TETRA) and Project 25 (P25) are two of the most adopted narrowband protocols for Public Safety and Industries with critical communications needs. Both standards have common characteristics that make them highly suitable for MC services, since they were designed with resilience and reliability at their core. However, considering its narrowband design, LMR systems cannot cope with the increasing PS traffic demand and the performance requirements of future use cases.

More specifically, the TETRA protocol is a digital trunked mobile radio standard developed to meet the need of traditional PMR user organizations in both Public Safety and commercial sectors (e.g., Transportation, Utilities, Government, Military, Oil & Gas, etc.). This standard was developed by public safety and two-way radio industry experts together with the European Telecommunications Standards Institute (ETSI) to ensure that TETRA devices provide secure, reliable, and instant voice and data communications in critical environments. This standard offers worldwide coverage (in more than 100 countries) and TETRA networks have typically 2 x 5 MHz FDD capacity ensuring 28.8k bps, however with some strategies it can go up to 691.2 kbps in an expanded 150 kHz channel.

The P25 protocol is a user-driven suite of standards developed for interoperable LMR systems to provide digital voice and data communications systems suited to public safety and first responders. This protocol was initiated by the Association of Public Safety Communications Officials (APCO) and developed by the Telecommunications Industry Association (TIA), strongly implemented in North America. Using this protocol, emergency responders can exchange critical communications across agencies and jurisdictions due to its standardized interfaces between the various components of the LMR systems emergency responders' use. It has a data transfer rate of 4.6 kbps, which is very slow considering modern standards and requirements.

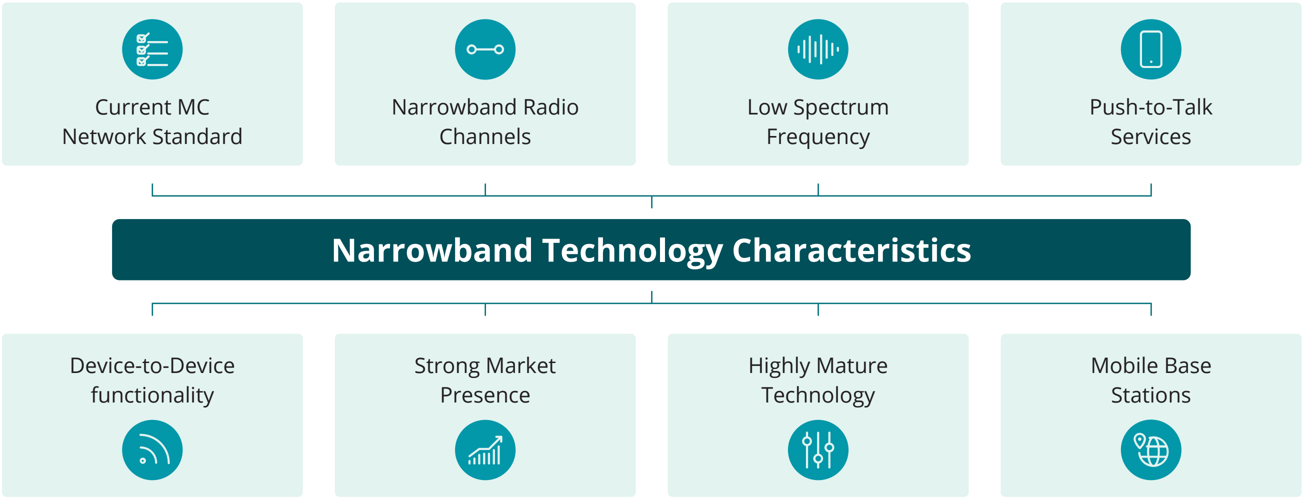

Current MC Network Standard
Narrowband Radio Channels
Low Spectrum Frequency
Push-to-Talk Services
Narrowband Technology Characteristics
Device-to-Device functionality
Strong Market Presence
Highly Mature Technology
Mobile Base Stations

Figure 5: Narrowband technology characteristics

Typically, both TETRA and P25 operate with lower frequencies, going below 400 MHz. This allows higher coverage per site/cell than with traditional commercial technologies and presenting features, such as standalone solutions, to work when backhaul link or Device-to-Device (D2D) communication fails.

Both TETRA and P25 are efficient and reliable technologies to establish voice communications, yet these have low data throughputs making them un-suitable to support the new data-driven needs of today's customers.

Narrowband System Limitations

Low Data Rates	Low data rates in comparison with current standards
Traffic Prioritization	No available voice call and/or traffic prioritization
Algorithmic Usage	No self-organizing and/or self-healing algorithms
No Improvement Margin	It has reached its maximum functionality and performance peak
Use Cases	Limited ability to enable new use cases
Frequency Usage	No frequency re-use margin to deploy new sites in some cases

Figure 6: Narrowband technology system limitations

Transitioning to broadband technologies such as LTE/5G is extremely important and can be the answer to higher data transfer rates, allowing several new use cases that could leverage PSA actions on field beyond current capabilities. The new use cases that could be enabled by LTE/5G data transfer rates will be able to significantly increase the situational awareness, either on field or on dispatch offices, supporting the decision-making process by sending more streams of information (possible use cases to be further discussed on this document).

Market Outlook

In accordance with "The Insight Partners", dating from July 2022 the mission critical communication market is expected to grow from US$ 17.03B in 2022 to US$ 27.87B by 2028; it is estimated to grow at a CAGR of 8.6% in the same time period. [3]

Source: [3]

4. 5G and its role for Critical Infrastructure

a) 5G Unprecedented Capabilities

Over the last few years LTE wireless technology has been deployed in some countries allowing the introduction of new (broadband based) capabilities for MC communications. Nonetheless, 5G is set to go much further in supporting the mission critical needs of industries and enterprises - far beyond just an increase in throughput. The fifth generation of mobile communication is based on a new network architecture that enables an outstanding performance and a revamped set of new features. It operates in three distinct spectrum bands – low, mid, and high frequency bands – ranging from 450 MHz to 100 GHz, which enables the expansion of the referred system capabilities. This large amplitude of spectrum usage is essential to build coverage in lightly populated areas, while simultaneously providing city-wide high capacity, both essential to the success of the MC environment. Additionally, new ways of communication, like 5G non-terrestrial networks (NTN), are being standardized and trialed, which also brings benefits to potential MCC use cases and coverage.

Besides providing efficient broadband capabilities, 5G networks will offer advanced measures for building ultra-reliable networks that deliver low latency, while simultaneously serving the needs of massive machine-type communication for sensors to better manage and control physical assets, enhancing the efficiency and quality of the PSA operations.

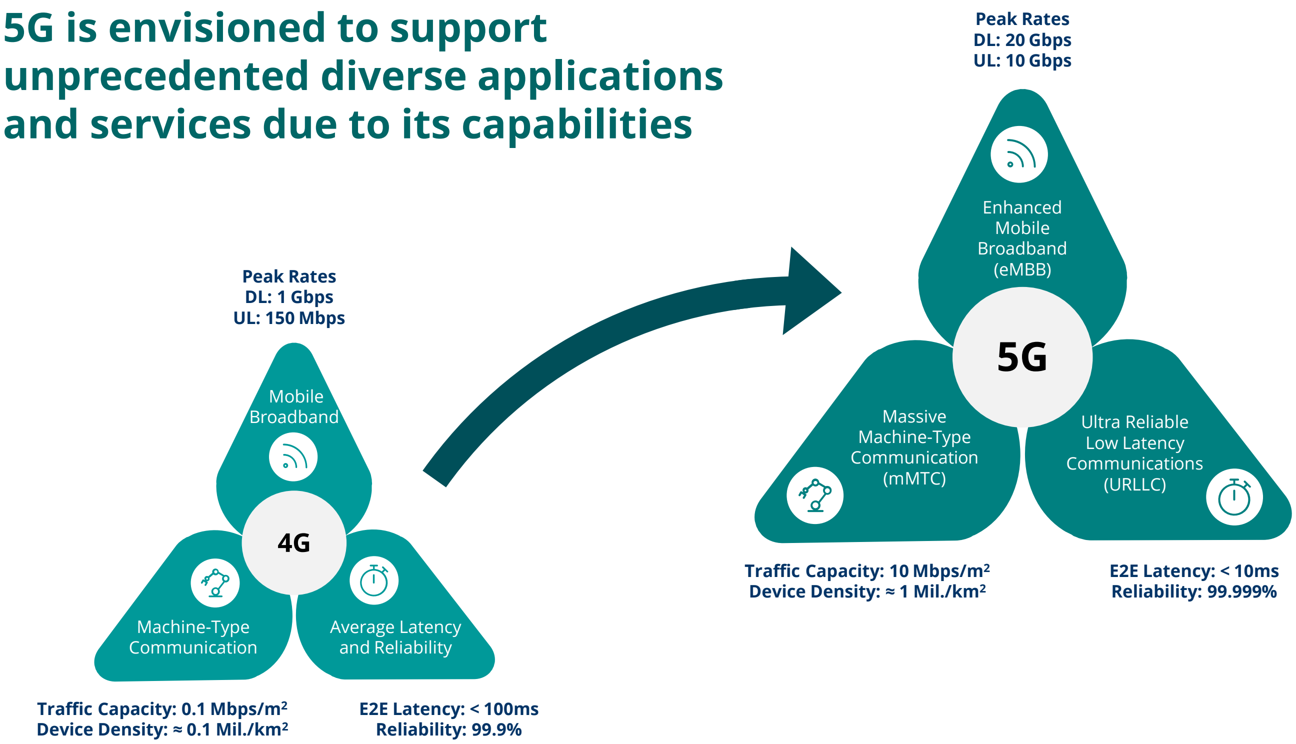

5G is envisioned to support unprecedented diverse applications and services due to its capabilities
Peak Rates
DL: 1 Gbps
UL: 150 Mbps
Mobile Broadband
4G
Machine-Type Communication
Average Latency and Reliability
Traffic Capacity: 0.1 Mbps/m²
Device Density: ≈ 0.1 Mil./km²
E2E Latency: < 100ms
Reliability: 99.9%
Peak Rates
DL: 20 Gbps
UL: 10 Gbps
Enhanced Mobile Broadband (eMBB)
5G
Massive Machine-Type Communication (mMTC)
Ultra Reliable Low Latency Communications (URLLC)
Traffic Capacity: 10 Mbps/m²
Device Density: ≈ 1 Mil./km²
E2E Latency: < 10ms
Reliability: 99.999%

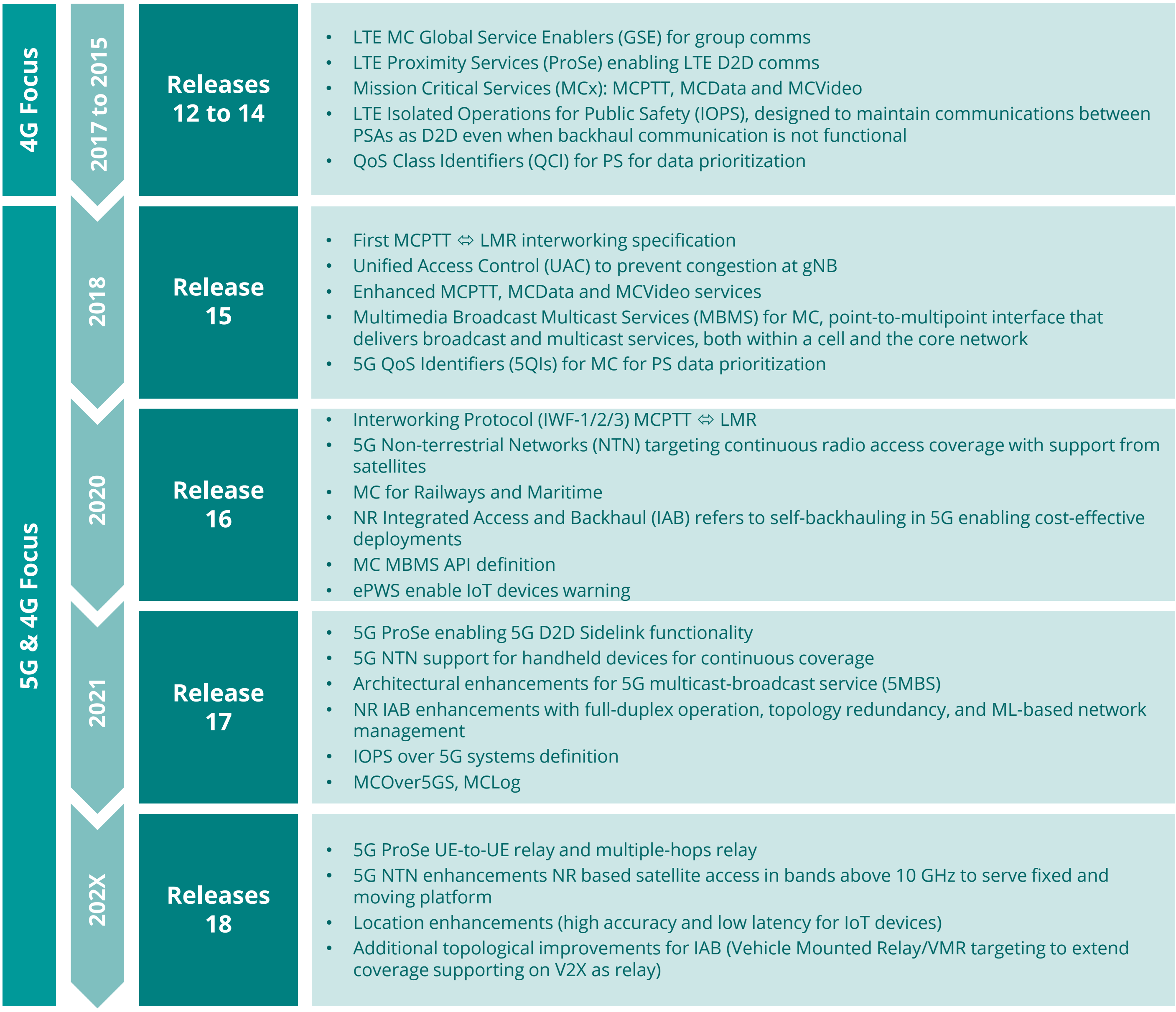
Figure 7: LTE and 5G technology capabilities

b) 3GPP Releases

3GPP (Third Generation Partnership Project) is an industry collaboration that manages the underlying standards for the on-going mobile communications systems like LTE, 5G and beyond. Each time a feature is designed for one specific release it enters into a development pipeline across vendors for it to be released commercially some years later. Since 2012, 3GPP has introduced and enhanced several MCC broadband solutions and delivered those features across several 3GPP Releases.

> The alignment with the 3GPP standards provides an improved ecosystem, with a more efficient interoperability that allows smoother inter-system migrations and system upgrades. Being compliant with this standardization is crucial to prevent system functionality fragmentation and security problems.

Some of the main features related with Mission Critical Communications were highlighted below in a non-exhaustive fashion:



4G Focus	2017 to 2015	Releases 12 to 14	• LTE MC Global Service Enablers (GSE) for group comms • LTE Proximity Services (ProSe) enabling LTE D2D comms • Mission Critical Services (MCx): MCPTT, MCData and MCVideo • LTE Isolated Operations for Public Safety (IOPS), designed to maintain communications between PSAs as D2D even when backhaul communication is not functional • QoS Class Identifiers (QCI) for PS for data prioritization
5G & 4G Focus	2018	Release 15	• First MCPTT ⇔ LMR interworking specification • Unified Access Control (UAC) to prevent congestion at gNB • Enhanced MCPTT, MCData and MCVideo services • Multimedia Broadcast Multicast Services (MBMS) for MC, point-to-multipoint interface that delivers broadcast and multicast services, both within a cell and the core network • 5G QoS Identifiers (5QIs) for MC for PS data prioritization
	2020	Release 16	• Interworking Protocol (IWF-1/2/3) MCPTT ⇔ LMR • 5G Non-terrestrial Networks (NTN) targeting continuous radio access coverage with support from satellites • MC for Railways and Maritime • NR Integrated Access and Backhaul (IAB) refers to self-backhauling in 5G enabling cost-effective deployments • MC MBMS API definition • ePWS enable IoT devices warning
	2021	Release 17	• 5G ProSe enabling 5G D2D Sidelink functionality • 5G NTN support for handheld devices for continuous coverage • Architectural enhancements for 5G multicast-broadcast service (5MBS) • NR IAB enhancements with full-duplex operation, topology redundancy, and ML-based network management • IOPS over 5G systems definition • MCOver5GS, MCLog
	202X	Releases 18	• 5G ProSe UE-to-UE relay and multiple-hops relay • 5G NTN enhancements NR based satellite access in bands above 10 GHz to serve fixed and moving platform • Location enhancements (high accuracy and low latency for IoT devices) • Additional topological improvements for IAB (Vehicle Mounted Relay/VMR targeting to extend coverage supporting on V2X as relay)

Figure 8: 3GPP releases roadmap and feature highlights. Source: [4]

Proof of this continuous cycle of design and delivery is, for instance, the forementioned 5G access networks enabled by satellites: it has been on Release 17 from 2021 and the first vendor to implement it on its UEs was Apple in a partnership with GlobalStar, owner of a constellation of satellites. Further features dedicated (or not) to PS MCC will continue to be rolled out during the next Releases. It is worth to mention that standardization of a 3GPP Release usually takes 1 to 3 years, so it is evolving all the time, however it also means that the actual availability of compliant products is later than the year mentioned in the figure above.

Not fully tied with 3GPP releases but being a joint effort from 3GPP and GSMA, Network Equipment Security Assurance Scheme (NESAS) framework was developed and has been maintained to assess network component security. The purpose of this framework is to prevent fragmentation of the security requirements and testing by providing a global baseline for security providing the required tools for testing.

c) 5G Innovative Features and their Role in Mission Critical Communications

To foresee the role that 5G will play in the MC environment, it is important to understand the impacts that some of its innovative features will generate, and their main advantages for the Public Safety field.

Apart from the more generalist capabilities, such as higher data rates, lower latencies and enhanced connectivity, this technology has several specific attributes that are developed or are under development and promise great improvements in comparison with PS-LTE and LMR narrowband technologies.

Opposing to LMR technologies, 5G (as well as LTE) is driven by several interests beyond PS or BCC (e.g., commercial Mobile Network Operators/MNOs, 5G private networks, PS itself) making them an ever-evolving technology with new features being added each Release, unlike LMR technologies which have reached its peak performance. Those Releases are well defined across a roadmap of features to develop.

Key 5G architectural features that will enhance MCC applications		Main advantages for MCC
Isolated Operation for Public Safety (IOPS)	With backhaul link damaged preventing the connection to the Core Network the site will still operate and enable communication between all UEs within site coverage	Enhances reliability of the network by enabling communications. LMR technologies have Local Fallback Mode solutions as well
Non-Terrestrial Networks (NTN)	Targeting at ubiquitous coverage for communications or some applications, where satellites can be used to enable LTE/5G access networks coverage	Continuous terrestrial coverage that will help to enhance both network availability and resilience for MCC
Proximity Services (ProSe)	Refers to the features enabling short range D2D, Side-Link and relaying options for UEs network with limited or non-existent network coverage	Enhances network resilience by enabling communication without coverage, or in a network failure situation, it is available for LMR with higher range due to lower frequency and higher transmit power
Multimedia Broadcast and Multicast Services (MBMS)	This services are being developed to enhance group-based communications by improving broadcast and multicast messaging systems	Creates new services such as public warning systems for PSA and enhances the efficiency of group communications
National Roaming	If the PS MNO adopts LTE/5G it will use the same technology as commercial MNOs and therefore upon agreement the PS UEs can roam into commercial MNO network if limited or non-existent coverage is available from PS network	If adopted, it will increase network reliability and availability by being able to roam into multiple networks from commercial MNOs to PS MNO
Unified Access Control	Represents an access barring mechanism introduced in the NR for selectively block new access requests originated at the UE side when in congestion scenarios	Reduces signaling and processing in gNB, ensuring network stability during high traffic loads
Integrated Access and Backhauling (IAB)	IAB refers to wireless backhaul using the same frequency and antenna available on site (in-band) or a second frequency and antenna (out-of-band), it is meant for temporary backhaul deployments	Can be used to recover backhaul links damaged during for instance wild-fires with in-band mode of operation. Additionally, both LMR and 5G have microwave and satellite links to replace physical backhaul
Mission-Critical Push-to-Talk (MCPTT)	MCPTT enables voice communication services between a pair of users or a group of several users, it has been enhanced during time from Release to Release	Enables one to one or group calls under MCC scope, this functionality is also present on LMR systems
Interworking Function (IWF)	Being LMR systems widely deployed and its transition being only possible on a gradual fashion, having interoperability between LMR and LTE/5G will ease its transition to LTE/5G	IWF will allow a progressive phaseout of LMR UEs, and a progressive acclimatization to the new technology being deployed (LTE or 5G)

Figure 9: 5G key architectural features and its impact for MCC. Source: [5]

There is much more to 5G than just these new features. There are architectural changes with benefits that could extend to MCC and enable new use cases:

Network Slicing enables the creation of specific, logical, and dedicated end-to-end slice over CSP (Communication Service Provider) network. Instead of the prevailing notion of a single and monolithic network serving multiple purposes, it allows to build logical networks on top of a common and shared infrastructure. Network slicing in 5G will enable specific slices targeted to for instance to some governmental entities with higher priority, Network-as-a-Service (NaaS) or dedicated slices with appropriate QoS for video-surveillance for instance.

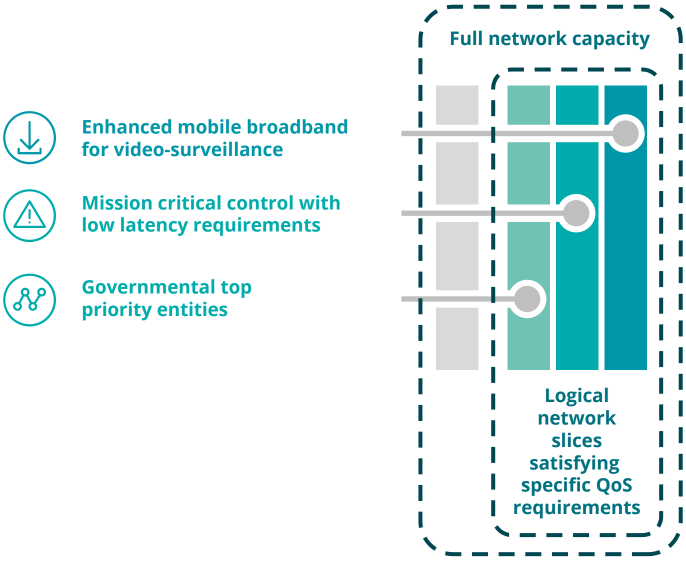

Full network capacity
Enhanced mobile broadband for video-surveillance
Mission critical control with low latency requirements
Governmental top priority entities
Logical network slices satisfying specific QoS requirements

Figure 10: 5G Network Slicing to meet specific QoS network requirements and enabling Network as a Service

Multi-Access Edge Computing (MEC) is an architecture paradigm that provides computer and storage capabilities by bringing the network resources closer to end-users. It represents an architecture that proposes several geographically distributed nodes that are located closer to the end user than the Central Data Centers, reducing the physical distance between the end-user and the network processing infrastructure. 5G uses this type of network to drastically reduce latency, making 5G MEC nodes a viable solution to enable several MC latency sensitive use cases.

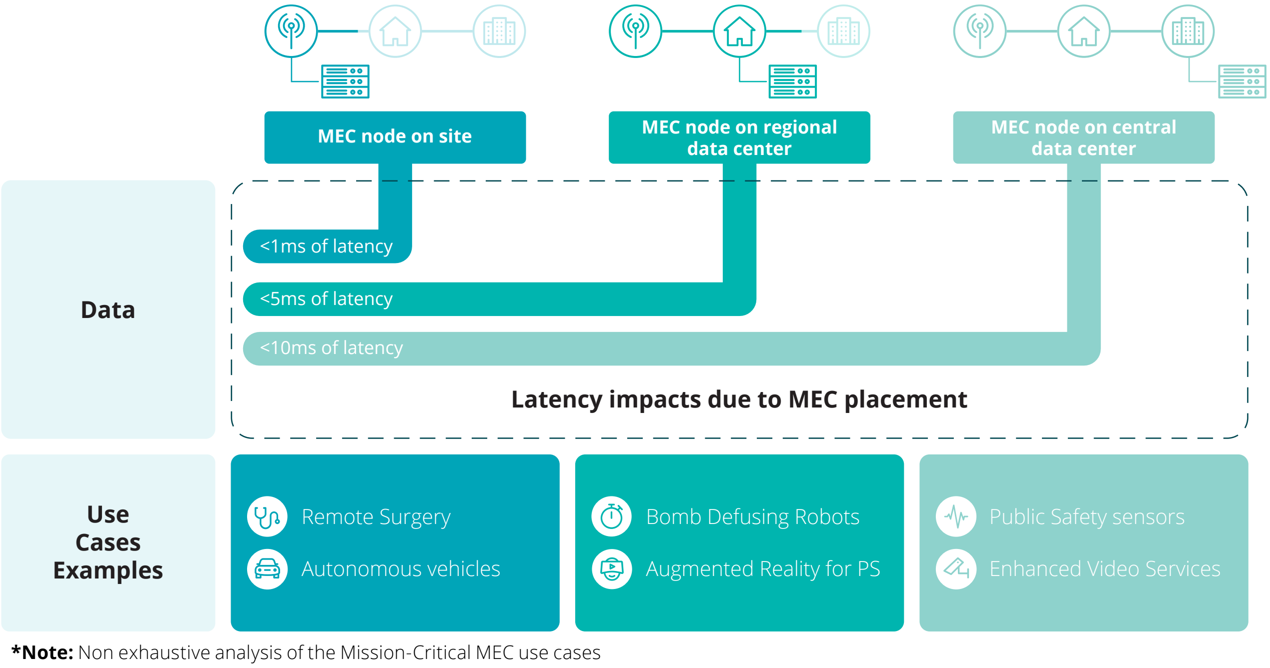


Figure 11: Multi-Access Edge Computing (MEC)

5. LTE/5G Public Safety Network Deployment Models

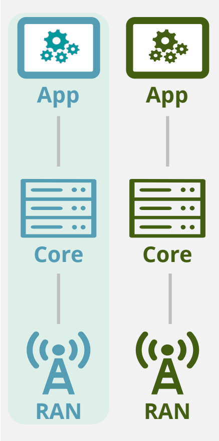
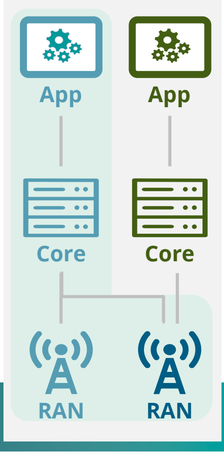
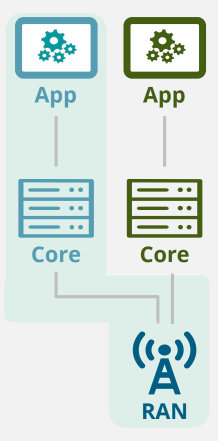
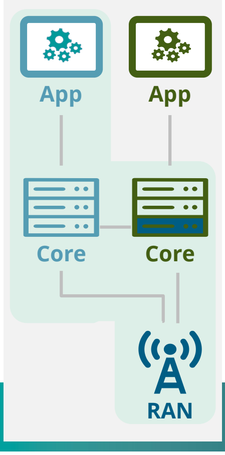
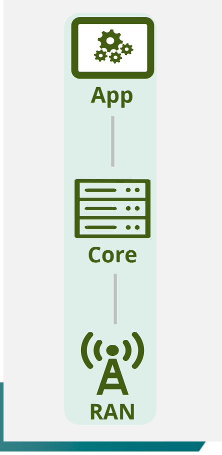
Deploying a nationwide Public Safety network is a massive investment for a country and unlike for LMR active elements could be shared between/with MNOs, this opens a viable opportunity to reduce the investment burden by entering a sharing agreement with a commercial MNO.

Another benefit of partnering with a commercial MNOs is that such operators usually provide significant indoor coverage unlike current LMR systems which often struggle with limited indoor reception. Beyond cost and coverage there are some risks to assess when entering is such agreements:

Timeframe for the Agreement	Entering and leaving sharing agreements with commercial MNOs are long-term commitments. Leaving a sharing agreement encompasses having to re-engineer all network which is cost-inefficient and could lead to disruptions on the service.
Network Admission Control	During emergencies or large scale events, there can be a high demand for mobile services and mobile networks can experience congestion. Emergency voice and data services need to have access priority and preferential treatment over non-mission critical communications ensuring a reliable communication mean for PS operations.
Secure Special Coverage Needs	Emergencies and large scale events can happen outside the coverage area provided by mobile networks and private radio networks, secure 100% coverage will be virtually impossible. It is then fundamental to secure flexible and displaceable coverage solutions like “Cells on Wheels” to provide emergency coverage capabilities in remote areas.
Commercial MNOs are Private	Commonly, commercial MNOs are private entities and some exposed on the stock market, this means that a government could rely in a partnership with a commercial MNO that can end up being sold to a foreign country alongside part of the PS network.
Devices	Several factors need to be considered on device development and availability, like spectrum bands, 3GPP compliance and dual-connectivity support. Price will be volume dependent and devices will need to meet PSMB requirements.
Network Hardening and Reliability	Performance and reliability of public networks need to be reinforced to secure Mission-Critical requirements. Extended Battery backup capacity, site redundancy and coverage reinforcement, backhaul bandwidth extension or site physical security need to be careful planned and executed.
Competition	MNOs with higher footprints will be better placed for a partnership to deploy PS networks, also, when renovating partnerships agreements MNO lock-in could be a risk, this could lead to higher prices when establishing contracts.
Regulatory and Spectrum	Regulation clarification on 400 MHz and 860 MHz spectrum bands availability and usage restrictions will be fundamental to align with MNO service availability on those bands and how to manage and leverage new bands availability.

Figure 12: Shared infrastructure with MNOs: Risks

The sharing models enabled by 3GPP are the following ones ranging from fully owned to fully deployed over a commercial MNO and depending on whether a dedicated frequency is available or not. A direct consequence is that with lower number of shared elements the price will rise, as well as the control over network, increasing the number of shared elements will lead to lower control but higher cost-effectiveness:

Nomenclature	Government lead network	Multi Operator Radio access network	Multi Operator Core Network	Secure FMVNO with dedicated core Network	Commercial lead network
Network Deployment					
Cost vs. Network Control	Highest Cost and Highest Control				Lowest Cost and Lowest Control
Description	The MCC network and the public network are implemented in a separate way. Passive elements such as the sites and the Transport Network can be shared in order to reduce the total cost of the network implementation.	The public network RAN is used to enhance MC network coverage, although the MC operator also has dedicated RAN components. Apart from the RAN, there are no shared components between both network.	The PS network RAN is entirely shared with the public network, meaning that there are no PS dedicated RAN components. Apart from the RAN, there are no shared components between both networks, including the Core.	The MC operator enters in agreement with MVNO in order to have access to their services. MCC network has a dedicated Core interconnected with the MVNO Core and another operators RAN.	The Public Safety network is implemented on top of the Public Network. Both the RAN and the Core are properties of the MNOs. Network slicing can be used to create a slice with resources dedicated exclusively to MC.
Spectrum Attribution	Use of Public Safety dedicated spectrum and/or commercial spectrum			Exclusive use of commercial spectrum	

Legend: ■ Public Safety Operator assets ■ Operator/ MNO assets ■ Shared assets □ Public Safety Network Components

Figure 13: Shared infrastructure with MNOs: Deployment/Sharing Models. Source: [6]

Entering sharing agreements has the disadvantage of constraints in the access to the sites, which can add a layer of complexity to the O&M (operations and maintenance) layer of the network and its associated costs.

Nonetheless, end-to-end security, especially in shared deployment models using a MORAN/MOCN or MVNO approach built on open interfaces and architectures, remains a challenge with the need to combine several network components not necessarily under the same operator control.

6. Status and Outlook: Global Public Safety Network Deployments

As mentioned in previous chapters, a key factor to have successful emergency operations is a reliable and always available communication network enabling real-time access to critical information and communications. The adoption of mobile broadband solutions will enable new possibilities to support advanced use cases and new MC services (e.g., MCVideo, MCData), as this will enhance situational awareness during PS operations.

The transformation of legacy public safety communications systems to 3GPP LTE/5G broadband networks is a worldwide trend. It comes with the added benefit of using the technology adopted by commercial MNOs, which means that significant investments are already planned and re-enforced by the existence of a roadmap. The transformation of the PS sector is being showcased by the implementation and successful launch of next generation PS networks in several countries, namely:

> Current MCC migration trend has been to move to PS-LTE, older and stable technology. Yet, PS-NR will deliver enhanced capabilities and longer-term viability. This immediately will translate in higher security for public safety agents.

UK – Emergency Services Network (ESN)

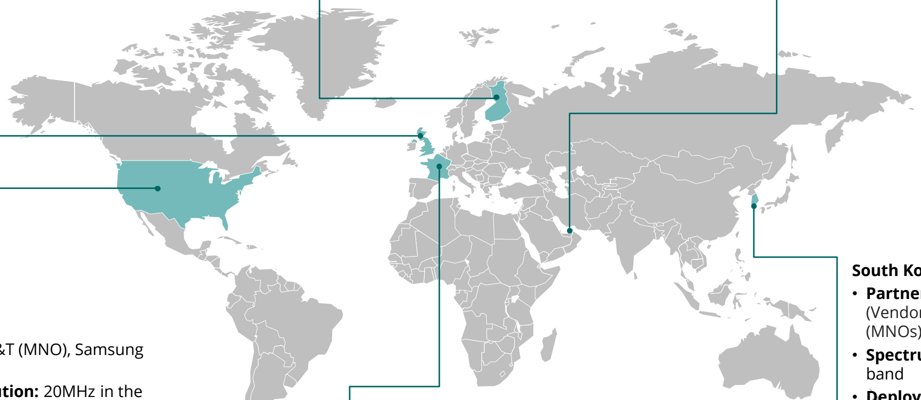
- **Partnerships:** Motorola (MC-PTT Vendor and Integrator) and EE (MNO)
- **Spectrum Attribution:** 800 MHz band
- **Deployment Option:** Commercial
- **Release Year:** 2024-2025
- **More info:** This network is being hardened by EE and UK's Home Office is deploying new 292 4G sites for enhanced coverage on remote locations. At this point it is still not available for PSA.

Finland – Erillisverkot

- **Partnerships:** Ericsson (CN Vendor) and Airbus (MC-PTT Vendor) and Elisa (MNO, RAN)
- **Spectrum Attribution:** Dynamic spectrum usage
- **Deployment Option:** MOCN
- **Release Year:** 2023-2025
- **More info:** VIRVE 2.0 is being developed to replace VIRVE (based on TETRA), MC-PTT solution is going to be provided by AIRBUS.

Dubai – Needa

- **Partnerships:** Nokia Solutions and Network (NSN)
- **Spectrum Attribution:** 700 MHz
- **Deployment Option:** Government (dedicated)
- **Release Year:** 2020
- **More info:** This solution relies in a fully owned government PS-LTE network (with RAN and Core Network).



South Korea – SafeNet

- **Partnerships:** Samsung (Vendor), SK Telecom and KT (MNOs)
- **Spectrum Attribution:** 700MHz band
- **Deployment Option:** MOCN
- **Release Year:** 2018
- **More info:** This network offers connectivity to first responders from over 330 public safety organizations.

USA – FirstNet

- **Partnerships:** AT&T (MNO), Samsung (IWF Vendor)
- **Spectrum Attribution:** 20MHz in the 700MHz band
- **Deployment Option:** MOCN
- **Release Year:** 2018
- **More info:** AT&T can use PS dedicated spectrum for commercial purposes but when there is capacity congestion, PS users have priority access. 5G available throughout AT&T in some regions but it is for data only, voice remains on LTE with defined priorities. National roaming is active.

France – ACMOSS

- **Partnerships:** 2 FR MNOs
- **Spectrum Attribution:** 700MHz band
- **Deployment Option:** MVNO
- **Release Year:** 2024-2025
- **More info:** The network will use the infrastructure from two MNOs for increased coverage and reliability setting up one MVNO, it is going to build its own Core network. Currently in bidding phase to later proceed for deployment.

Figure 14: Non exhaustive view on global activity concerning MCC over LTE or 5G. Source: (7) (8) (9) (10) (11) (12)

Concerning the sharing models, so far mainly two schemes were adopted throughout the Global Public Safety landscape, MOCN or MVNO. Despite both models require some hardening to meet PS Service Level Agreement (SLA), that are contractually defined. Commercial MNOs can for instance build new sites to reach nationwide coverage. Both models represent at the expense of network control a more cost-effective solution than deploying a fully dedicated network.

The MOCN sharing model states that no RAN hardware is needed to deploy the PS network and therefore only the Core Network is to be built by the government/ PS authorities, plus the mobile backhaul links (which can be leased). Furthermore, this model is especially suitable when dedicated PS spectrum is available.

Additionally, MVNO approach is another widely adopted infrastructure sharing model suitable in case no dedicated PS spectrum is available, however it represents a more complicated setup than the MOCN. In the traditional case, MVNO possesses part of the Core Network (not owning the part of the Core Network that controls the RAN), which means that sensitive information could be visible to the commercial MNO (e.g., location and call activity). To prevent this, instead of using the roaming interface, further Core Network elements could be added making it a Secure MVNO, which is closer to the MOCN model and it is strongly related with the will of the PS authority to keep its information fully separated or not from the commercial MNO.

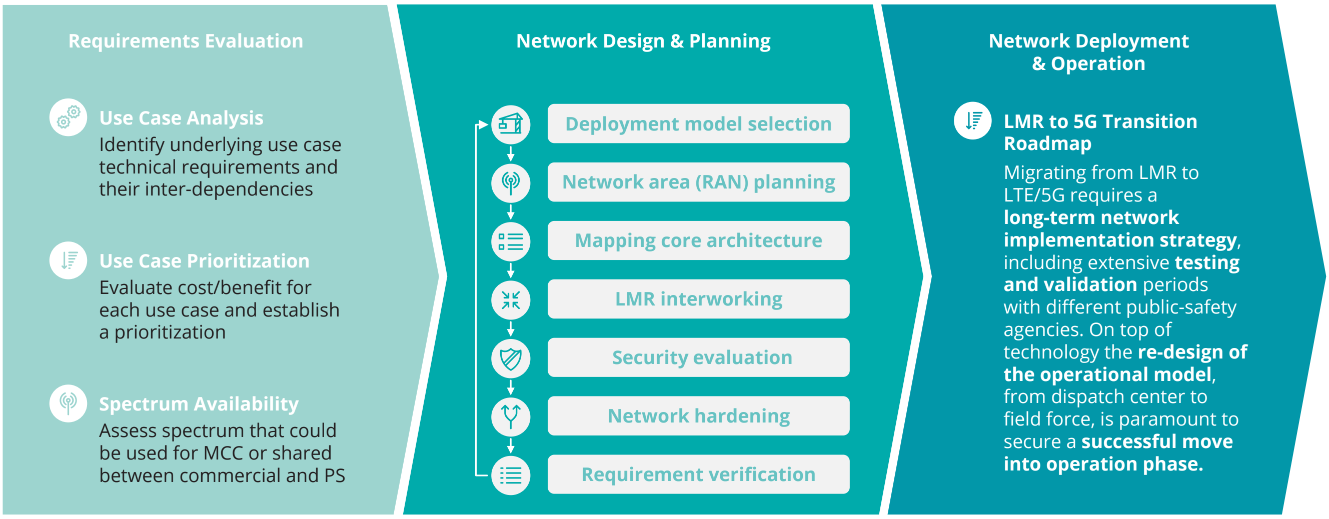
It is important to refer here that FirstNet from USA used 700 MHz but used it as a shareable asset to make the contract with AT&T more attractive, so when it was not being used for PS purposes it was made available commercially.

Usually, the dedicated frequencies for PS are in the range of 700 MHz and 800 MHz, which provide improved coverage on wider territories. In Russia the PS network used 450 MHz which is within 3GPP one of the lowest frequencies possible to adopt but the one capable of providing even better wide area coverage.

7. Path to Success: Transition from legacy LMR to 5G

Like the migration from analogue to digital LMR, the transition of public safety networks towards a next generation cellular network architecture will require operational processes that can, beside availability and reliability, ensure coverage and, especially, ensure fulfillment of security requirements from an end-to-end perspective. Dedicated planning, an agreed roadmap and clear focus on the actual user, as well as foreseen use cases, will help to mitigate potential transition risks.

The transition itself will require detailed analysis of the foreseen use cases with respect to the engaged parties and needed resources, to enable them nation-wide. With that information identified it is possible to enter in a planning phase to select the most suitable deployment model and to define and agree on a corresponding transition roadmap.



Requirements Evaluation

Use Case Analysis
Identify underlying use case technical requirements and their inter-dependencies

Use Case Prioritization
Evaluate cost/benefit for each use case and establish a prioritization

Spectrum Availability
Assess spectrum that could be used for MCC or shared between commercial and PS

Network Design & Planning

- Deployment model selection
- Network area (RAN) planning
- Mapping core architecture
- LMR interworking
- Security evaluation
- Network hardening
- Requirement verification

Network Deployment & Operation

LMR to 5G Transition Roadmap
Migrating from LMR to LTE/5G requires a **long-term network implementation strategy**, including extensive **testing and validation** periods with different public-safety agencies. On top of technology the **re-design of the operational model**, from dispatch center to field force, is paramount to secure a **successful move into operation phase.**

Figure 15: From Use Cases to the Transition Roadmap

Rather than being just an incremental migration, this is a generational leap with completely new architecture enabling new services with additional broadband capabilities, supported by enhanced user equipment and different operating concepts. The figure above highlights the main phases, which must be considered during the transition execution, some specific challenges along this process will be discussed on the next pages.

a) Use Case Evaluation and Technical Capabilities

From a global perspective for Mission Critical Communications, the change from legacy voice-centric use cases to mission critical broadband and data-centric services has already started. The availability of broadband and multi-service capabilities ensures advantages; however, it implies challenges that must be considered during network planning and especially during the transition phase.

Broadband capabilities, lower latency and specifically Edge Computing cannot just be added separately.

Assessing the use-cases to deploy will undoubtedly impact network planning and design (e.g., consider MEC nodes in critical areas to analyze CCTV video and trigger warnings).

● Higher Demand
○ Lower Demand

Example MCx Service Requirements

	RADIO COVERAGE	THROUGHPUT DEMAND	LOW LATENCY	GROUP COMMUNICATION	E2E SECURITY
MCPTT Mission Critical Push To Talk	●	◔	◔	●	●
MC DATA & MC Video Mission Critical data and video availability for further support (possible real-time sharing)	●	●	●	◕	●
Body Worn Video / Cameras Body Worn Video (BWV) / Body Worn Cameras (BWC)	●	●	◔	◔	●
Dashcams Connected dashboard cameras / car digital video recording	◕	●	◔	○	●
Tactical Bubbles ad hoc-type non-public, mobile communications networks	●	●	◑	●	●
Geolocation Tracking & identification of connected electronic devices	●	◔	◕	○	◕
Connected Infrastructure Information sharing (data, video, etc.)	●	◕	◑	○	●
Connected Equipment Information sharing (data, sensors, etc.)	●	◔	◑	○	●
Connected Vehicles Information sharing (data, video, etc.)	◕	◕	◑	○	●
Automated Guided Vehicles (AGVs) Autonomously driving or remote controlled vehicles	●	◕	●	○	●
Autonomous Drones Drones flying under mobile network connectivity – possibly Beyond Visual Line of Sight (BVLOS)	●	●	●	○	●
Autonomous Robotics Autonomously moving or remote controlled robots	●	◕	◕	○	●
Virtual Reality / Augmented Reality Improved reporting of additional information	●	●	●	○	●
3D Maps & Indoor Location 3D maps and further indoor guidance for first responders	●	◑	◕	○	◕
Smart Surveillance Video processing at the edge with AI support	●	●	●	○	●

Figure 16: Typical Service Requirements for MCx use cases

For the selection of the most suitable deployment model, it is crucial to understand the interdependencies of all foreseen use cases and their underlying technical requirements to ensure readiness of the required infrastructure. It is also important to know the needs and capabilities of future control rooms and dispatch solutions, i.e., it is highly recommended to involve vendors of such products in an early stage of the transformation journey.

b) LMR Interworking with Mobile Networks

LMR systems are field-proven and in scenarios where LMR is successfully deployed and widely used, this (legacy) technology is going to coexist for many years beyond the introduction of 5G based MCC. Reasons vary from (limited) 5G coverage to non-replaceable, dedicated user equipment, e.g., in vehicles. 3GPP and the related LMR SDOs (e.g., TCCA/ETSI for TETRA) support such requirements with the consideration of the so-called Interworking Function (IWF).

The IWF should bridge the different technologies for those use cases, which are implemented in both network architectures, e.g., in case of TETRA this is Push-to-Talk and Data services, however some other common services like geo-location and group management are also supported. The standardization is a split approach: 3GPP defines the specifications and protocols for the 3GPP part (i.e., LTE and 5G networks) and the LMR part needs to be covered by the corresponding LMR organizations.

Figure 17.

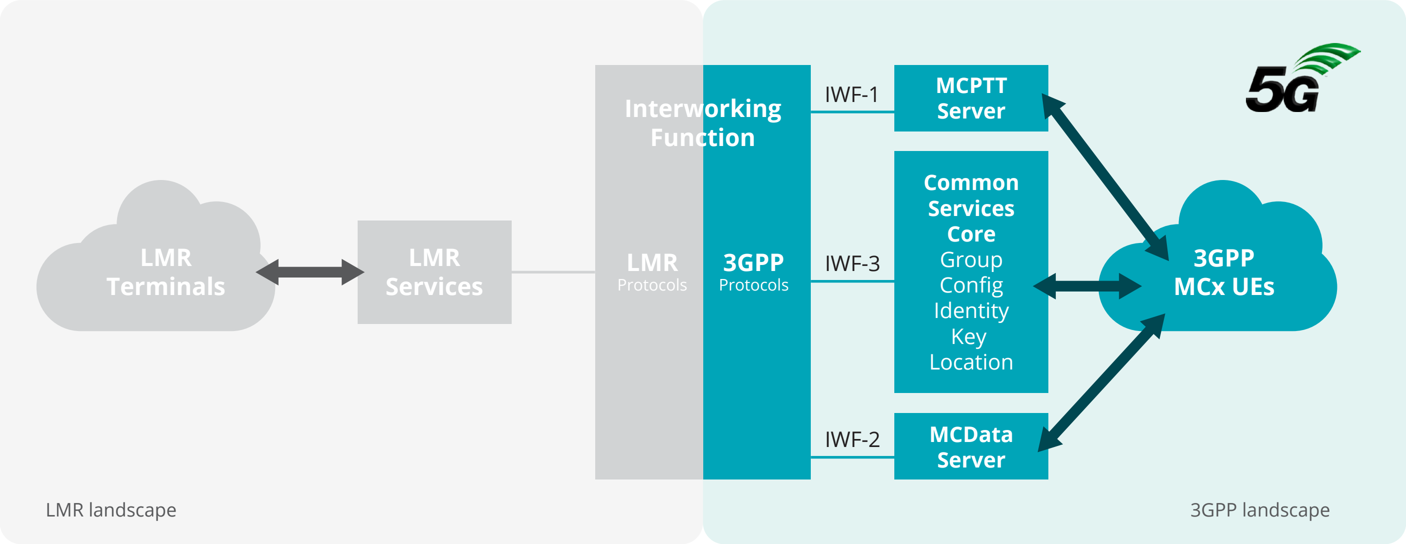


Figure 17: LMR/3GPP Interworking Function

Despite the undoubtful benefit that technical standards ease interoperability, the reality might require proprietary approaches to overcome the interworking challenge. First, the standardization is still progressing and not all incumbent LMR vendors are willing to implement the Interworking Function. Secondly, with respect towards IWF capabilities, the differences between TETRA and P25 must be considered, e.g., both systems use different voice codecs, which has impact on transcoding.

In general, the foreseen co-location of the IWF with the LMR system is a case-by-case decision, which needs to be taken into account in a very early project phase. If a standardized IWF is not feasible, other interworking technologies, such as (RoIP) gateways, need to be evaluated. However, this approach might cause additional efforts (e.g., double provisioning) or risks (e.g., vendor lock-in due to proprietary solutions).

LMR interworking with mobile networks can ease migration effort at several levels, however the transition is a split effort 3GPP defines the specifications and protocols for the 3GPP part while the LMR part needs to be covered by the corresponding LMR organizations

c) Dual Connectivity Devices

Depending on the adopted migration strategy, the gradual traffic transition from one network technology (TETRA resp. P25) towards the other (LTE/5G) could take several years, leading to longstanding projects.
Therefore, interoperability and dual connectivity devices are essential to support this process and allow the seamless transition between narrowband and broadband systems. At this point, since mostly PS-LTE networks were deployed until know, only dual-connectivity LMR and PS-LTE devices are present in the market.

Having dual-connectivity devices available will allow the device to connect to both systems depending on its geographical availability across the nation and quality of signal. Using this approach, the PSA will only carry one device capable of connecting to LMR and LTE (dual connectivity with 5G is expected later). When the transition process is finished and the LMR system is eventually unplugged, these devices will still be fully functional in the broadband networks and, therefore, the investment on DC-UEs will not be lost when LMR is in End-of-Life stage.

There are several LMR to LTE dual-connectivity devices already available in the market from well-known suppliers of MCC UEs, such as Motorola or Airbus. Dual-mode LMR/MCPTT devices will help to close the gap between old and new technologies. It is expected devices will begin to deliver 5G-supported mission-critical push-to-talk services to first responders soon.

It is still worth mentioning that dual connectivity devices will have access to both networks (LMR and LTE/5G), so those will benefit opposing to LTE/5G devices from an extended device to device range.

d) Network Hardening – Vulnerabilities Mitigation

Saving lives and avoiding harm are the main tasks for PSA. Therefore, the used communication networks and its equipment must follow very stringent requirements in terms of reliability, especially for radio coverage and security. With respect to the selected deployment model, there is a clear trend to share certain network equipment with commercial MNOs. Moreover, it is even possible to partner with MVNOs to share a certain level of equipment, however this could impose higher risks due to the missing direct access to the corresponding network infrastructure.

Until today, commercial MNOs designed their networks with profitability at its core and, as a consequence, rural areas often have no adequate coverage. Therefore, entering a sharing agreement and achieving MCC required full coverage is possible, nevertheless it will most likely require further network enhancements.

Especially with respect to possible Open RAN architectures, the fulfilling of additional PSA requirements might become a challenge since it will entail extensive testing to demonstrate that it is able to cope with high demand scenarios.

To create reliable MCC architecture networks, so called network 'hardening' techniques will be necessary to mitigate possible vulnerabilities, considering the following elements:

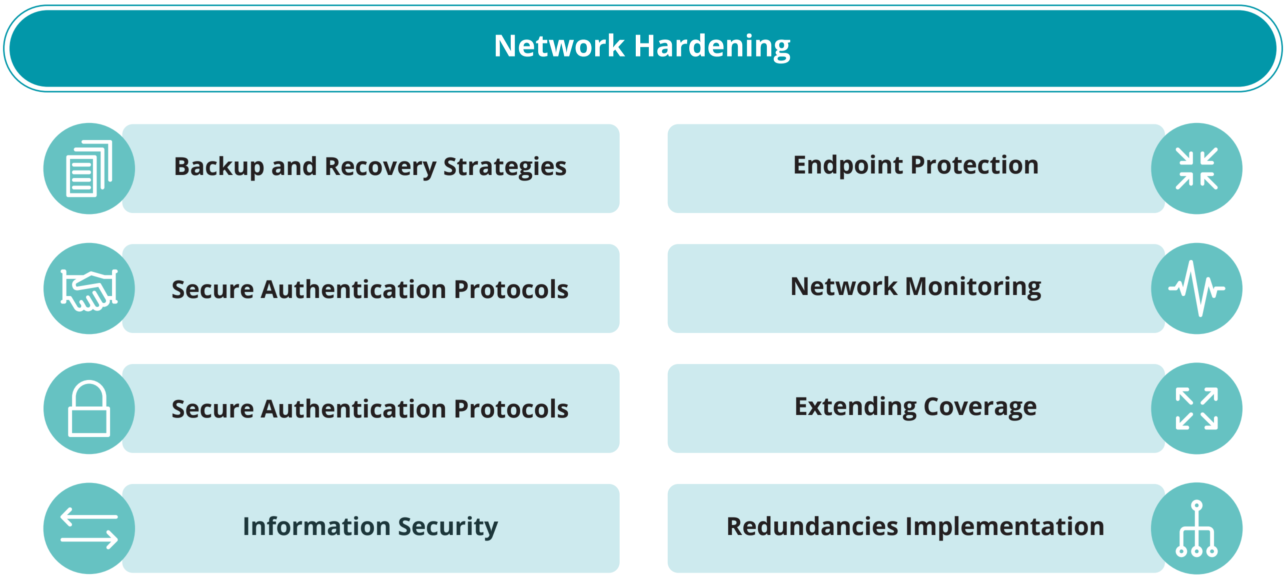

Network Hardening
Backup and Recovery Strategies
Endpoint Protection
Secure Authentication Protocols
Network Monitoring
Secure Authentication Protocols
Extending Coverage
Information Security
Redundancies Implementation

Figure 18: Network Hardening Focus Domains

As a general approach, for each used network entity it will be required to document existing network design and configuration, identify and remediate security vulnerabilities, as well as reliability concerns and, finally, define safeguards against future vulnerabilities.
Additionally, in order to assure to respect the end-to-end perspective and even allow service availability in case of backhaul incidents, physical network redundancy should be considered by using redundant core and RAN elements and/or extended battery backups, as well as features that increase network resilience, such as IOPS functionalities, or with respect to upcoming 5G releases and new possibilities, Non-Terrestrial Networks (NTN) or UE-to-UE relay features.

Roaming from PS-NR (or PS-LTE) networks to commercial networks can have a meaningful impact on reliability and indoor coverage

Coverage and Mobile Sites

- Requirements on coverage levels are high for MCC networks since they are meant to serve all territory rather than all population. Therefore, when opting for a sharing agreement with a commercial operator some network coverage hardening will be needed and could be government or PS entity lead, some points are worth considering:Coverage per cell/site is higher on LMR systems since those rely on lower frequencies (approximately 400 MHz), while commercial MNOs typically work from 700 MHz onwards, which means that a higher number of sites is needed to deploy a broadband technology.

- Commercial networks have lower levels of coverage than a typical implementation of a MCC NW, however it is important to notice that they are designed to have higher indoor coverage.

- 5G NTN should be utilized as fallback as soon as the technology and devices are available.

Relying on commercial MNOs infrastructure with a well-designed network coverage hardening will lead to a broad coverage, both indoor and outdoor, since commercial MNOs have denser and heterogeneous networks.

UK is building its PS network in conjunction with EE's network (UK based MNO), which had approximately 19.000 sites, from those 700 needed to be upgraded to 4G and further 292 sites are being deployed to achieve near 100% nation-wide coverage. [13]

Source: [13]

In case of natural disasters, terror attacks or similar unexpected events, the network infrastructure might be destroyed or non-usable. In such cases, flexible, active elements are needed to set up a PS and/or (public) communication network in short term, based on an existing variety of moveable equipment.

The fleet of deployable solutions (more than one hundred) includes ground-based vehicles such as Cell on Wheels (COWs) and heavy-duty Satellite Cell on Light Trucks (SatCOLT), as well as the use of drones - Flying COWs (Cell on Wings), that are essentially tethered drones equipped with a satellite dish, fiber connections and Band 14 connectivity. Additionally, blimps can also be used as an advanced tethered aerostat platform, which hovers in the air and establishes communication links . First backpack-based solutions with foldable antennas are available today, which can be carried by a single person and are able to create ad hoc LTE/5G/LMR networks to cover a specific area.

(National) Roaming

In most cases it is expected that a single operator will not be sufficient to provide full network coverage for a foreseen region. For further coverage and increased network resilience, roaming agreements with national or international providers (in terms of cross border engagements) will play a fundamental role in hardening the network experience – especially with respect to backup capabilities in case of network blackouts.

8. Conclusion

Looking at the future of Mission Critical Communications, and especially at the growing number of possible use cases enabled by broadband networks, which can enhance the situational awareness and the operation efficiency. There is then the appetite for evolution, to move to a network capable of enabling a safer environment in Public Safety operations in response to these needs, LTE based network planning and deployments have been started to offer public safety-oriented services beside TETRA and P25.

From a technological standpoint, 5G and even LTE network solutions are already able to deliver sufficient bandwidth today to support the required broadband needs on MCx services. Additionally, PS networks which rely on MCC networks are not the only drivers of development, BCC networks (e.g., transportation, oil, gas) are also driving innovation and development which will lead to further features being deployed over time. Furthermore, 3GPP based networks have some characteristics that made then highly interesting to MCC networks, the ability to enable national roaming, work with dual-connectivity devices or enhance indoor coverage. However, irrespectively of the benefits, it is required to look at the mandatory characteristics of a public safety network to have broadband communication services and new features enabled: full coverage, security and reliability are the key challenges to overcome during the transition phase towards MCx broadband.

Meeting all the required characteristics for a broadband MCC network is not a straightforward path, whether it is supported on commercial MNO network with the needed hardening or government lead, some points are always to be considered:

- Outlining the migration and modernization strategy towards PS broadband;
- Calculating business cases for the selected deployment model against a set of SLAs and requirements;
- Defining the right deployment model for each case, by assessing potential benefits and risks from partnering with commercial MNOs;
- Pinpointing benefits, risks, and mitigation actions for the identified risks;
- Support in defining hardening actions to meet the required network SLAs;
- Plan a tailored migration aiming to modernize the network without disrupting service availability (since each network to deploy is different and carries its own requirements);
- Evaluate possible use cases to implement on the PS network.

Besides the benefits of broadband communication and new features in cellular network architectures, it will be a challenge to ensure the required security level, particularly in shared network deployments. 5G networks are more laid out to an open architecture, nevertheless all entities must be considered for the security evaluation respecting the required network hardening processes and the end-to-end perspective, including selected devices and corresponding application layers for monitoring and control.

What to expect in the coming years?

To fulfill the growing demand for broadband communication in public safety networks it will be required to finally changeover to cellular networks. Although the feature list in 3GPP standardization for LTE/5G is outranging TETRA/P25 capabilities, it will take several years to have the already standardized features and corresponding devices available in real networks to allow a full transition.

As seen in the LMR market, MCC networks exist for a very long time after a technology is proven and accepted. This will lead to a broader selection of dual connectivity (LMR/3GPP) devices in the coming years to ease the migration. But also, Regulators will have the responsibility to assign the necessary frequency spectrums long-term to ensure the newly made investments are safe, and if sharing infrastructures agreements are done, then those should be on the long-term frame.

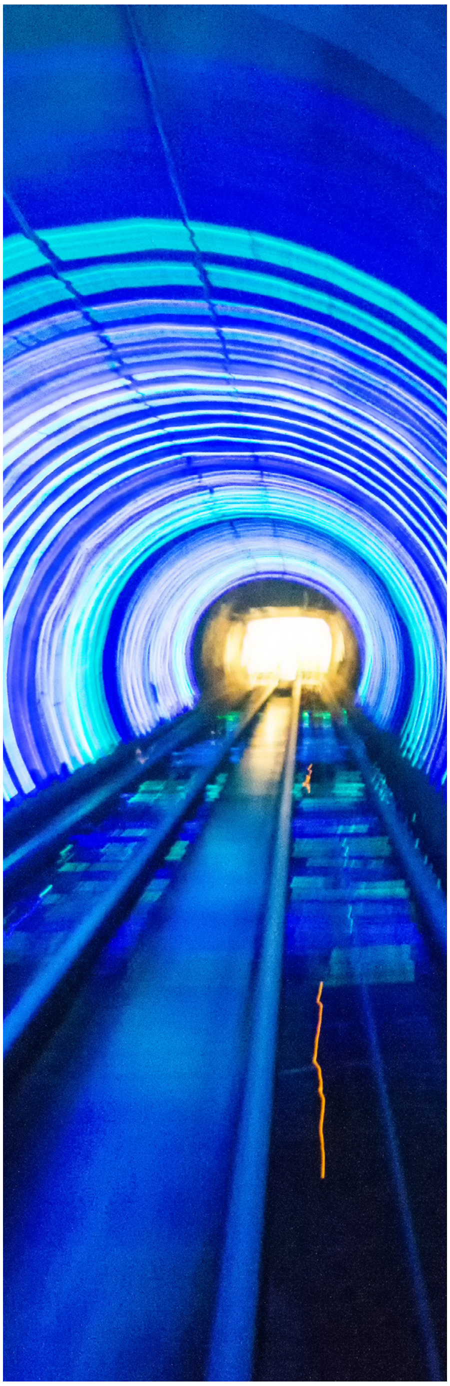
More specifically, due to the existing lack of full coverage in cellular networks, we will see hybrid network approaches using TETRA/P25 and LTE/5G networks in parallel with interworking functionality to fulfill present and future requirements until coverage is comparable and sufficient. Thereby, LMR networks can act as a backup to extend reliability if the user moves beyond LTE/5G coverage in border areas and beyond.

To further extent coverage and reliability, a national roaming agreement with multiple MNOs can be set up which will dramatically increase the PSA experience.

From a cost perspective, it is unexpected to see many solely "Government Lead Networks", using an independent LTE/5G network to provide mission critical broadband communication services completely hosted by a single operator.

Furthermore, the end-to-end perspective, especially with respect to security considering device and application availability, will be required for selecting the most suitable deployment models.

Long term, the subsequent use of LMR is not expected nor sustainable – as soon as the MCC features in existing cellular networks are mature, a switchover is then recommended.



Glossary

3GPP – Third-Generation Partnership Project

LTE – Fourth Generation of mobile communication

5G – Fifth Generation of mobile communication

5MBS – 5G Multicast and Broadcast Services

APCO – Association of Public Safety Communications Officials

BCC – Business Critical communications

CAGR – Compound Annual Growth Rate

CSSI – Console Subsystem Interface

D2D – Device to Device

DFSI – Digital Fixed Station Interface

DMR – Digital Mobile Radio

eMBB – Enhanced Mobile Broadband

ePWS - Enhanced Public Warning Systems

ESN – Emergency Services Network

ETSI – European Telecommunications Standards Institute

E-UTRAN – Evolved Universal Terrestrial Radio Access Network

FCC – Federal Communications Commission

FDD – Frequency Division Duplex

GBR – Guaranteed Bit Rate

IDC – International Data Corporation

IOPS – Isolated Operations for Public Safety

IoT – Internet of Things

ISSI – Inter-RF Subsystem Interface

IWF – Interworking Function

KT – Korea Telecom

LMR – Land Mobile Radio

LTE – Long Term Evolution

MC – Mission Critical

MCC – Mission Critical Communications

MCC NW - Mission Critical Network

MCPTT – Mission Critical Push-to-Talk

mMTC – Massive Machine Type Communications

mmWave – Millimeter Wave

MOCN – Multi Operator Core Network

MORAN – Multi Operator Radio Access Network

MVNO – Mobile Virtual Network Operator

NR – New-Radio

NTN - Non-Terrestrial Networks

O&M -Operations & Maintenance

P25 – Project 25

PMR – Professional/Private Mobile Radio

PoC – Proof of Concept

PPDR - Public Protection and Disaster Relief

ProSe – Proximity Services

PS – Public Safety

PSA – Public Safety Agents

PS-LTE – Public safety LTE

PTT – Push-to-Talk

RoIP – Radio over IP

SDO – Standards Development Organization

SKT – South Korea Telecom

SON – Self-Organizing Networks

TCCA – The Critical Communications Association

TETRA – Terrestrial Trunked Radio

TIA – Telecommunications Industry Association

uRLLC – Ultra-Reliable Low Latency Communications

V2X – vehicle-to-everything

References

[1]"Natural Disasters," Our World in Data, (2022). "Terrorism," Our World in Data, (2013)

[2]"Worldwide Private LTE/5G Wireless Infrastructure Market Set to Reach $8.3 Billion by 2026, According to IDC," Telecom TV, (2022)

[3]"Mission Critical Communication Market Size to hit $27.87Bn, Globally, by 2028," The Insight Partners, (2022)

[4] "Mission Critical Services in 3GPP," The 5G Standard, (2017)

[5] "Mission Critical Services in 3GPP," The 5G Standard, (2017)

"A guide for deploying and developing mission critical applications using broadband technologies," TCCA, (2022)

"Isolated E-UTRAN operation for public safety," Public Safety LTE, (2016)

"5G evolution: 3GPP releases 16 & 17 overview," Ericsson Technology Review Articles, (2020)

"Mission Critical Services Standards: Advancing Critical Communications Across Industries," Samsung, (2021)

[6] "Enabling intelligent operations with Mission Critical Networks," Ericsson, (2021)

"Migration to mission critical 4G and 5G," Ericsson, (2021)

[7] "Migration to mission-critical 4G and 5G," Ouest France, (2020)

[8] "Empowering America's first responders with FirstNet," FirstNet

[9] "Emergency Services Network: overview," The Home Office, (2023)

[10] "Virve is becoming a broad-band service – this is how the development is progressing," Erillisverkot, (2021)

[11] "Nedaa CEO: Running reliable networks for critical operations," Intelligent CIO, (2019)
"Nedaa to Launch 4G LTE for Mission-Critical Applications," The critical communications review, (2019)

[12] "Samsung Powers World's First 3GPP-Compliant Nationwide Public Safety Network with MCPTT Service in Korea," Samsung Newsroom U.K, (2021)

[13] "The Public Safety LTE & 5G Market: 2022 – 2030 – Opportunities, Challenges, Strategies & Forecasts," SNS Telecom & IT, (2022)

Contacts

Sponsors

Pedro Sanguinho
Senior Manager
Deloitte Portugal
Global Telecom
Engineering Excellence
psanguinho@deloitte.pt

Hugo Santos Pinto
Associate Partner
Deloitte Portugal
Global Telecom
Engineering Excellence
hupinto@deloitte.pt

Philipp Deibert
Partner
Deloitte Germany
pdeibert@deloitte.de

Constantin Völkel
Director
Deloitte Germany
cvoelkel@deloitte.de

Authors

Miguel Ramos
Tech Senior
Deloitte Portugal
Global Telecom
Engineering Excellence
miramos@deloitte.pt

Afonso Carvalho
Tech Consultant
Deloitte Portugal
Global Telecom
Engineering Excellence
afocarvalho@deloitte.pt

Carolina Gonçalves
Tech Consultant
Deloitte Portugal
Global Telecom
Engineering Excellence
carolgoncalves@deloitte.pt

Volker Wittmann
Manager
Deloitte Germany
vwittman@deloitte.de

Mario Ruprecht
Senior Specialist Lead
Deloitte Germany
mruprecht@deloitte.de

Deloitte.

This communication contains general information only, and neither Deloitte Touche Tohmatsu Limited (“DTTL”) nor its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Accordingly, before deciding or taking any action that may affect your finances or your business, on the basis of this communication you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and therefore neither the issuer, nor DTTL or its network of member firms, related entities, employees or agents may be held liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication.