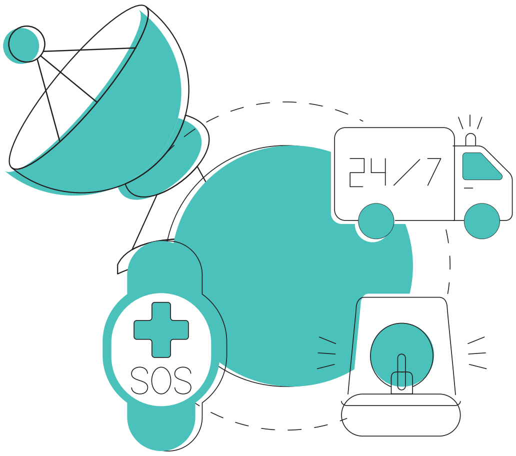
TOWARDS A FUTURE-PROOF MISSION CRITICAL COMMUNICATION ECOSYSTEM FOR PUBLIC SAFETY

Mission Critical communication systems and tools are a real lifeline for Public Safety emergency services. With this paper, Capgemini Invent aims to provide an overview and clear recommendations to support authorities in their transformation journey to evolve towards broadband Mission Critical communication solutions.

CONTENTS



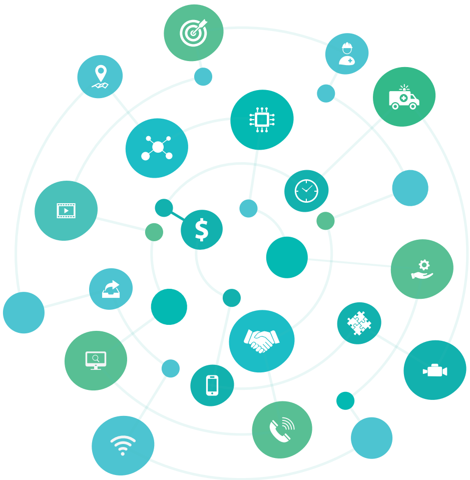
INTRODUCTION

Over the last few years, Public Safety teams, including first responders, have been confronted globally with crisis situations going beyond imagination. Terrorist attacks such as 9/11 or the terror attacks in Brussels and Paris increased the overall need to communicate in critical situations. This resulted in the saturation of the networks, coupled with possible interoperability issues between the first responders' units on the ground and crisis management centers. This made cooperation very difficult, if not almost impossible, thereby leading, in some cases, to the use of unsecured alternatives. Natural disasters such as flooding, forest fires or earthquakes cause massive damage to communication infrastructure, hence slowing down rescue operations at critical times, which may put many lives at risk.

The frequency and magnitude of those crises seem to increase, stretching the capabilities of the emergency forces and their communication tools to the maximum. Apart from these extreme situations, the police and emergency services are also confronted every day with situations where reliable communication is essential for their operations. In fact, communication is a real lifeline during interventions as the lives of not only citizens, but also those of first responders are directly at stake. As such, the **terminology "Mission Critical communications" refers to the communication systems used in operations where lives are possibly in danger and which require all possible technical and operational support.**

For decades, reliable narrowband voice-based systems have been implemented globally to support Public Safety's essential communication needs. However, technological evolutions and more advanced usage requirements are leading to the obsolescence of current Mission Critical technologies and are driving a shift towards a new paradigm – mobile broadband solutions. While voice applications remain paramount, data- and video-based applications are becoming increasingly important during crisis situations and day-to-day operations. Drones, robots, AIVs, video-images, AR/VR, AI and IoT devices, introduced in parallel with new network technology generations (i.e., LTE/5G etc.), can drastically enhance the situational awareness and the overall efficiency of operations. The newest 4G/5G mobile broadband solutions present themselves as a valid alternative to the currently narrowband systems as those have reached their limits and cannot support the new data-hungry applications. The evolution towards mobile broadband systems is a fundamental shift of the Mission Critical ecosystem, but it comes with radical and expensive choices that must be made.

Being confronted with such a shift in technology and user behavior is certainly a major challenge for the decision makers. But it is, at the same time, creating a window of opportunities to organize and implement a more up-to-date, performant, reliable, efficient, and future-proof Mission Critical communication approach. Being at a turning point, this is the right time to question the current organizational, operational, and technical models. In fact, the latter should be designed to ensure that the Mission Critical communication systems of the future really address the relevant requirements of all stakeholders in the ecosystem to fulfill current and future needs. In this document we provide insights on how to best approach the future Mission Critical ecosystem as well as the associated transformation challenges and opportunities.



MISSION CRITICAL SYSTEMS ARE THE LIFELINE OF FIRST RESPONDERS

When responding to an emergency call, first responders of Public Safety services must be able to communicate with each other and their dispatch centers effectively. This requires access to robust and reliable communication systems that are always available, no matter what may be happening. For this reason, high-quality "Mission Critical" communication systems were developed.

Mission Critical communications have been introduced and used by a variety of sectors, industries, and businesses (e.g., utilities & transport, road & rail, private security, etc.), but the most relevant use case is Public Safety or PPDR[1] (public protection and disaster relief) sector.

MISSION CRITICAL (MC) CONCEPT

The "Mission Critical (MC)" concept applies to communications that are highly reliable to be used during safety, security or emergency crisis management and prevention, when lives, environmental or social damage are at stake.

Communication solutions used by PPDR actors (often referred to as the "disciplines", "users", "services" or eventually "first responders" in this paper) are the backbone of the intervention process, and in many cases a real lifeline, for the people in distress and the responders themselves. As "Mission Critical", these communication systems must provide and ensure fast, reliable connectivity with maximum availability at anytime, anywhere and with the highest quality of service (QoS[2]).

Today, countries with a well-structured emergency and security response system have developed and are operating networks with reliable technologies, often based on dedicated infrastructure and spectrum. Nevertheless, the dedicated technologies used today are progressively reaching their end of life, or rather becoming obsolete as they cannot evolve to support the growing user requirements for mobile data services and mobile applications. Consequently, current Public Safety communication solutions are at a turning point as they must evolve toward other, more adapted, technologies. The new generation of mobile broadband network technologies (i.e., 4G, 5G, etc.), initially developed for commercial and industrial applications are becoming progressively more suitable for PPDR applications[3]. However, their development in this very specific segment is still quite new, many aspects and requirements must be considered to ensure that Public Safety disciplines have access to mobile broadband solutions with, at the least, an equivalent level of quality and services as what is being provided today.

KEY QUESTIONS

Which drivers are pressing for an evolution of current Mission Critical communications systems?

What opportunities and challenges arise from the use of 4G/5G technologies for Mission Critical communications?

How should governments and Public Safety authorities drive this transformation?

This paper aims at providing clear answers to such questions and supporting, by means of recommendations, decision makers as they plan for the evolution to next-generation communication systems.

[1] PPDR actors refer to all actors involved in the Public Safety sectors such as police forces, firefighters, medical & ambulance, defense & military, customs, security services, etc. to cite the most critical ones.

[2] QoS = Quality of Services

[3] Since the release 13 (R13) of the 3GPP mobile standards have included relevant functionalities for PPDR services, equivalent to those from legacy PMR/LMR systems, all relevant features for PPDR applications are considered to ensure the same functional of PMR/LMR legacy systems.

“Mission Critical” – to cope with extreme situations

DIMENSIONS	BUSINESS CRITICAL (BC)	MISSION CRITICAL (MC)
Design principles	Profitability, competitiveness, and sufficient reliability in most situations	Full redundancy, hardening, maximum reliability, priority, and preemption
Target audience	Commercial/industrial organizations, private users, leisure, etc.	Public safety actors and associated organizations
Network type	Commercial networks	Generally dedicated and hardened networks
Application scalability and functionality	Developments and evolutions follow or even drive the pace of the market	Need standardization before reaching MC level
Communication availability	Under reasonable or normal "critical" conditions	At all times (BC conditions + “operational” & “technical” crises)
Impacts in case of failure	Operations termination with economic value or sensitive information at stake	Risk of lives and important material damage at stake
Coverage	≤ 99.5% of the population	≥ 99.5% of the territory
Back-up time in case of electrical failure	≤ 2 hours	≥ 8 hours

In the field of mobile communication systems, there are three categories of usage differentiated by the objectives that their specific users want to achieve and the corresponding configuration requirements (in terms of end-user equipment, technology, network features, characteristics, standardization, etc.).

The Commercial segment targets commercial users for their everyday communication needs. At the other end of the spectrum, the Critical segment, including mainly Business and Mission Critical systems, requires mobile radio systems (incl. devices) which can provide secure and reliable communication in the most extreme or specific circumstances. In many sectors and industries, they are essential to ensure smooth running of emergency operations.

Business Critical systems generally serve organizations that must operate in an environment where there is significant economic value and/or sensitive information at stake.

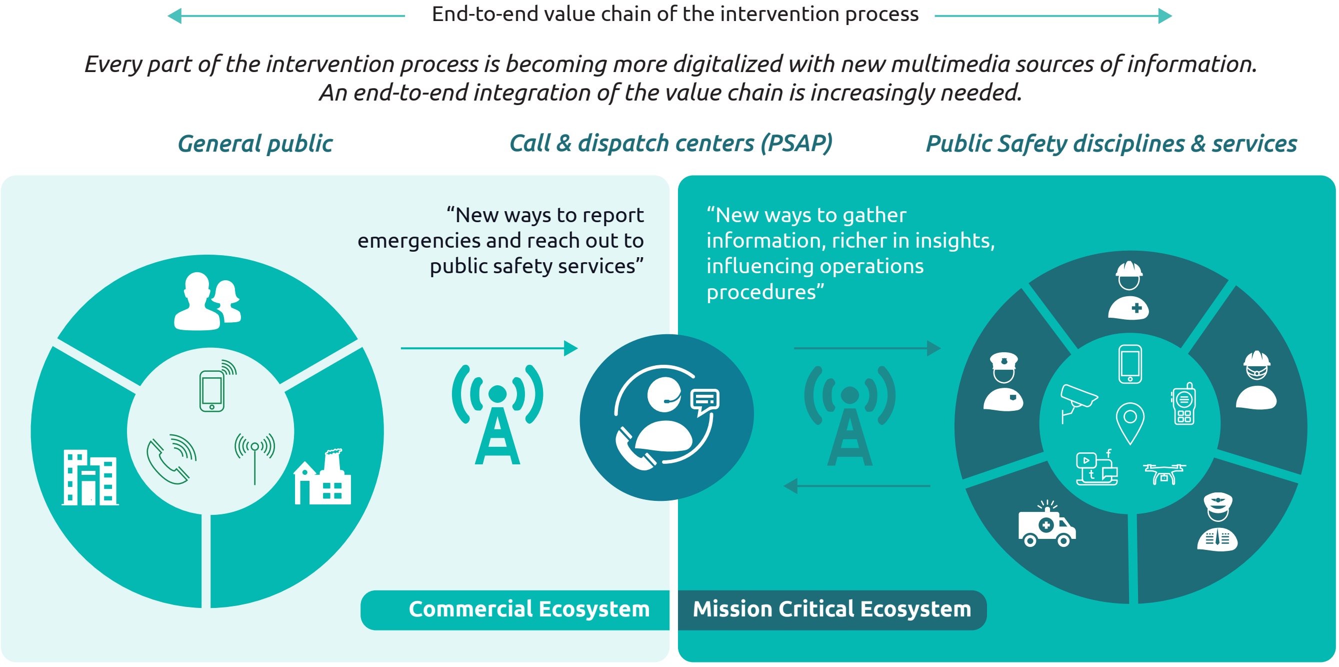
Mission Critical systems, however, were designed for missions where a failure may result in serious safety or security damage, injury, loss of life, or would significantly harm society or the environment. As such, their users are mostly made of Public Protection and Disaster Relief (PPDR) actors.

The key driver of critical systems in general, is to ensure the effectiveness and efficiency of systems in a crucial situation. Mission Critical systems have the safety & security of the society at their core, implying that profitability is set aside, prioritizing public interest above all.

DESIGNING MISSION CRITICAL NETWORKS

Mission Critical networks are designed to be operational and available in all circumstances even in the most extreme cases (i.e., network failure/shutdown, terrorist attacks, natural disaster, major accident, etc.); to do so, they include additional characteristics (i.e., enhanced coverage including temporary/tactical “bubbles”, back-up systems including deployable systems, hardening, prioritization mechanisms), and features developed to fulfill the users’ very stringent communication requirements.

Emergency response – an integrated process involving many stakeholders


End-to-end value chain of the intervention process
Every part of the intervention process is becoming more digitalized with new multimedia sources of information.
An end-to-end integration of the value chain is increasingly needed.
General public
Call & dispatch centers (PSAP)
Public Safety disciplines & services
"New ways to report emergencies and reach out to public safety services"
"New ways to gather information, richer in insights, influencing operations procedures"
Commercial Ecosystem
Mission Critical Ecosystem

Many stakeholders are involved in an "intervention process": the general public, the Call & dispatch centers (also known as PSAP[1]) and the Public Safety disciplines, each needing to communicate with each other to ensure the efficient execution of operations. The general public, "upstream" of the process, makes emergency calls to call and dispatch centers or "PSAP" to trigger the intervention process. The PSAP analyses the situation and makes the appropriate decisions, dispatching the relevant teams and disciplines on the field (i.e., police forces, firefighters, medical teams, and ambulances, etc.). "Downstream" is the intervention itself, including all its actors[2]. The communication tools, systems, and infrastructure are the backbone of most operations, but they differ for each stakeholder group.

> *"A robust dispatch solution that is proven, well-integrated, and trusted, is important for Public Safety to begin considering full transition to broadband MC systems."*
>
> ***– FirstNet, USA***

The dedicated Mission Critical systems are used by the Public Safety disciplines during interventions or in day-to-day operations. The public reaches out to call centers through the commercial networks to communicate their emergency[3]. The PSAP then operates with fixed line connectivity and is integrated with both commercial and Public Safety networks.

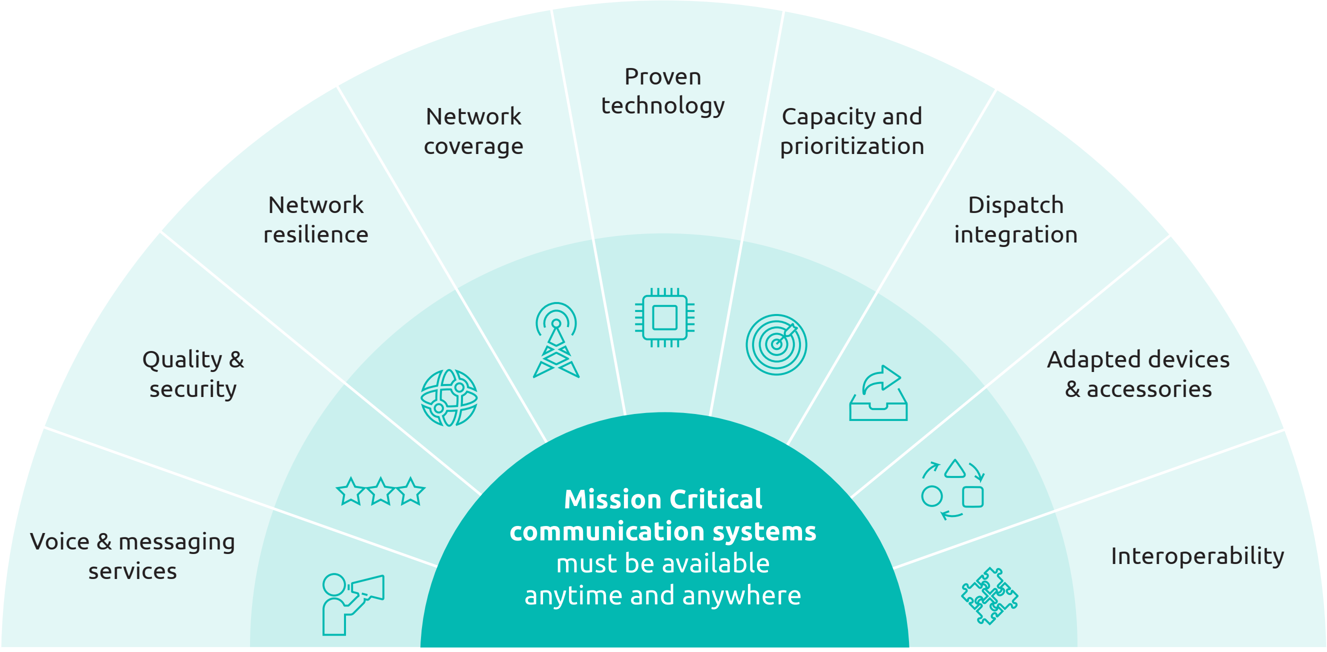
A complete end-to-end integration of dispatch solutions with Mission Critical communication systems is a prerequisite to ensure that Public Safety responders know what to do in every situation. Moreover, all tools and accessories used by each Public Safety discipline must also be completely integrated with the systems to ensure users are best equipped to fulfill their own mission. The weakest links of the value chain, however, are the commercial networks used by the population as they do not provide a similar level of reliability and robustness. Past experience has shown that it is not only critical to ensure communication amongst and between the different emergency and security services, but also between those services and the civilians in distress.

[1] PSAP: Public Safety Answering Point

[2] Note that this third group of stakeholders do not only include security & emergency services, but also services (such as customs, defense, etc.) that have different operational and communication needs.

[3] Some initiatives have been introduced allowing the population to share more information to the PSAP, increasing situational awareness at a small scale (i.e., 112 apps introduced in Europe).

Current systems - relying on narrowband technologies with voice and limited data services


Voice & messaging services
Quality & security
Network resilience
Network coverage
Proven technology
Capacity and prioritization
Dispatch integration
Adapted devices & accessories
Interoperability
Mission Critical communication systems must be available anytime and anywhere

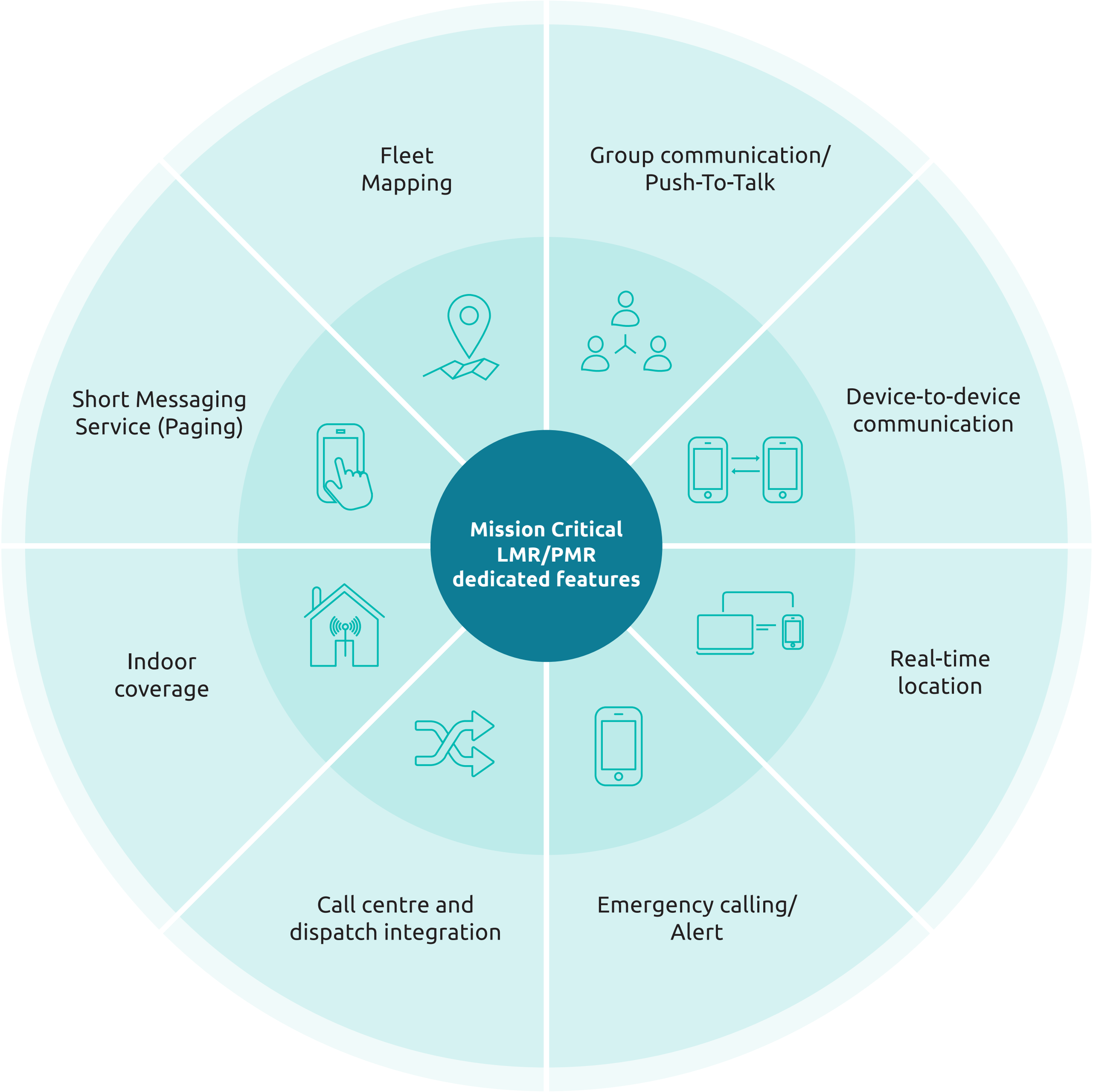
Connectivity solutions and technologies are evolving at a fast pace for commercial users. This can be attributed to the fast innovation cycle of the highly competitive telecommunication market. Public Safety communications, however, are not subject to the same competitive pressures. The networks used have been relying on stable and reliable technologies and infrastructures, historically different from the commercial ones as the latter did not comply with the "Mission Critical" requirements.

Mission Critical communication services have been traditionally based on dedicated networks, created from government initiatives. To this day, most Public Safety networks rely on PMR/LMR[1] systems and are based on proprietary protocols and technologies (i.e., TETRA, P25 and DMR, POCSAG or legacy analog technologies) which were specifically designed with resilience and security at the core. Such systems have allowed authorities to provide robust and reliable Mission Critical systems that can deliver voice and limited messaging services.

LMR/PMR systems are efficient and reliable in sharing information and managing field operations, and as such in fulfilling basic Public Safety service requirements. However, the technologies on which they rely cannot support new data-driven needs.

[1] PMR/LMR: private/land or mobile radio (depending on Europe or the US) are terms referring to a professional two-way mobile radio system, based on standards & dedicated protocols, developed for specific organizations.

Business models have also followed a dedicated approach with the service providers being, in general, governmentally controlled through independent organization(s) serving PPDR and related agencies. However, not all countries, have opted for a nationwide approach (unique central and dedicated organization and network). Some have chosen a decentralized approach with local networks[1]. This has shown its weaknesses as Public Safety users have repeatedly experienced interoperability and compatibility issues in various locations.


Mission Critical LMR/PMR dedicated features
Fleet Mapping
Group communication/ Push-To-Talk
Device-to-device communication
Real-time location
Emergency calling/ Alert
Call centre and dispatch integration
Indoor coverage
Short Messaging Service (Paging)

[1] For example, today in France, Switzerland, and US, where disciplines and/or local geographic areas manage and operate their own networks (TETRAPOL, TETRA and P25 respectively).

THE MISSION CRITICAL ECOSYSTEM IS AT A TURNING POINT

Worldwide, Mission Critical (MC) systems, differ slightly but they all follow the same basic “design principles”. This is also true for the future next generation of MC services. The shift towards the 4G/5G mobile broadband ecosystem seems inevitable, something which both Public Safety users and authorities agree upon. LMR/PMR standards and solutions have reached their functionality and performance limits and cannot evolve to deliver the broadband services that users will need in the future. In fact, mainstream mobile broadband solutions, conveyed through commercial networks, are already being used by Public Safety disciplines but do not support the required MC features, let alone the extended coverage and hardening. This means that today, first responders cannot rely on such solutions to communicate in the most critical events. Fortunately, the technologies and standards have evolved, now making it possible to adapt 4G/5G networks to the stringent requirements of Mission Critical services. As such, the future Mission Critical systems will address a larger ecosystem of actors (network, device, software providers, etc.).

Evolution of technologies and users’ requirements

Narrowband LMR/PMR technologies offer a high level of reliability, security, and resilience for voice-based communications and limited data capacity (mainly short messages on pagers). However, this ecosystem is limited in terms of suppliers and networks interoperability (national and international). Additionally, market dynamics tend to show a progressive end of life for the current systems – within the next 10 to 15 years. As such, equipment suppliers are expected to stop supporting “legacy” technologies, competencies, know-how, and devices to focus their activities on new broadband technologies.

In parallel, commercial broadband networks have been massively rolled-out by public network operators, reaching very high level of coverage and democratizing mobile data & video usage. The development of 5G networks will further drive digital innovation and foster the development of new use cases and new devices (IoT wearables, cameras, sensors, drones, etc.). Public Safety users follow the same trends by using commercial mobile broadband networks to fulfill new needs (video streaming, image, location sharing, etc.). Going forward the next generation of Mission Critical communication solutions (MCX[1]) will be gradually implemented on 4G/5G[2] technologies with open standards defined by the third-generation partnership (3GPP)[3].

> *“There is no doubt that Public Safety disciplines will increasingly rely on mobile broadband applications. The whole ecosystem needs to shift. But all key features are not yet available, e.g., device-to-device.”*
>
> ***– SWISSCOM, Switzerland***

[1] Mission Critical broadband standards and protocols now exist and are called “Mission Critical services” and referred to as MCX, short for MC-Voice, MC-Data and MC-Video services.

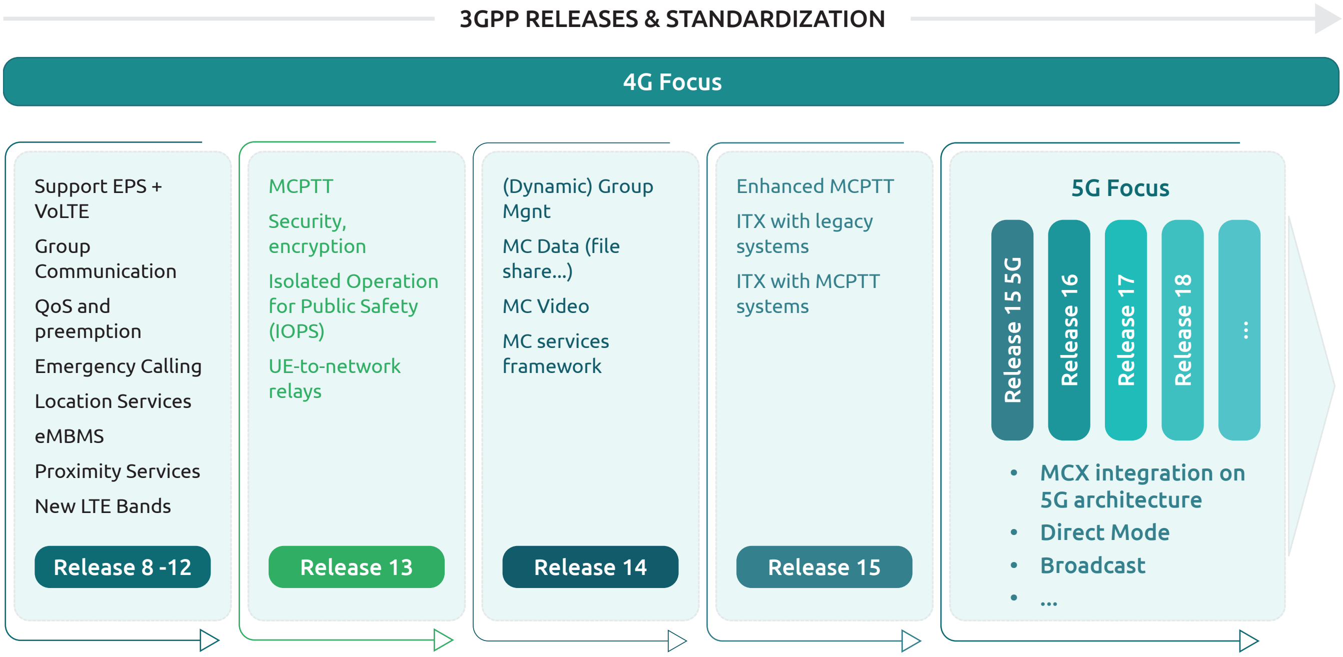
[2] It is important to note that currently, not all necessary Public Safety features are supported by mobile broadband networks. But it is now a matter of time. New 3GPP release programs are now focusing on 5G, IoT and Public Safety Mission Critical features.

[3] The terms 4G and 5G are labels attributed to technology generations. They are a continuous stream of 3GPP defined releases. In addition, 3GPP have produced Mission Critical Specifications “MCS releases” since March 2015. Moreover, Mission Critical communication is an even more relevant aspect of 5G. Release 17, being the start of MCX over 5G, ensures support of Proximity Services covering the Direct Mode feature of TETRA, the support of Broadcast/Multicast requirements, Interworking Function, security, etc.

The time where specifically designed and dedicated systems and technologies were absolutely needed to fulfill the Mission Critical requirements is coming to an end. The 3GPP standardization (since R13) has brought the prioritization mechanism enabling the support of a first set of MC services over 4G networks. This is opening the possibility of running Public Safety critical applications over commercial networks, hence leveraging the high coverage of public mobile 4G networks. Nonetheless, specific add-ons and requirements, in terms of infrastructure (e.g., coverage, hardening etc.) and features, must be implemented to turn these public networks into reliable, high-performing, secure Mission Critical communication systems.

The implementation of broadband critical features opens a new market, not only driven by the Public Safety sectors, but also by industries for which 5G will digitalize the processes and operations. The global Mission Critical communications market revenue will grow from $13.9B in 2019 to over $20B by 2025[1]. The broadband critical communications industry will be used mainly for ensuring Public Safety. For the global Public Safety LTE market, a CAGR of 18% in the next 5 years is expected ($6B in 2020 to $12.8B in 2025)[2]. North America currently leads the market, followed by Europe and Asia Pacific. The high potential of this emerging market will bring many opportunities and highlights the inevitable shift toward the 3GPP broadband Mission Critical ecosystem.

> *"All users have a TETRA device but also a smartphone and almost all have a tablet. The users need broadband services and go to commercial providers."*
>
> ***– SWISSCOM, Switzerland***



3GPP RELEASES & STANDARDIZATION

4G Focus

Support EPS + VoLTE
Group Communication
QoS and preemption
Emergency Calling
Location Services
eMBMS
Proximity Services
New LTE Bands
Release 8 -12

MCPTT
Security, encryption
Isolated Operation for Public Safety (IOPS)
UE-to-network relays
Release 13

(Dynamic) Group Mgnt
MC Data (file share...)
MC Video
MC services framework
Release 14

Enhanced MCPTT
ITX with legacy systems
ITX with MCPTT systems
Release 15

5G Focus

Release 15 5G
Release 16
Release 17
Release 18
...

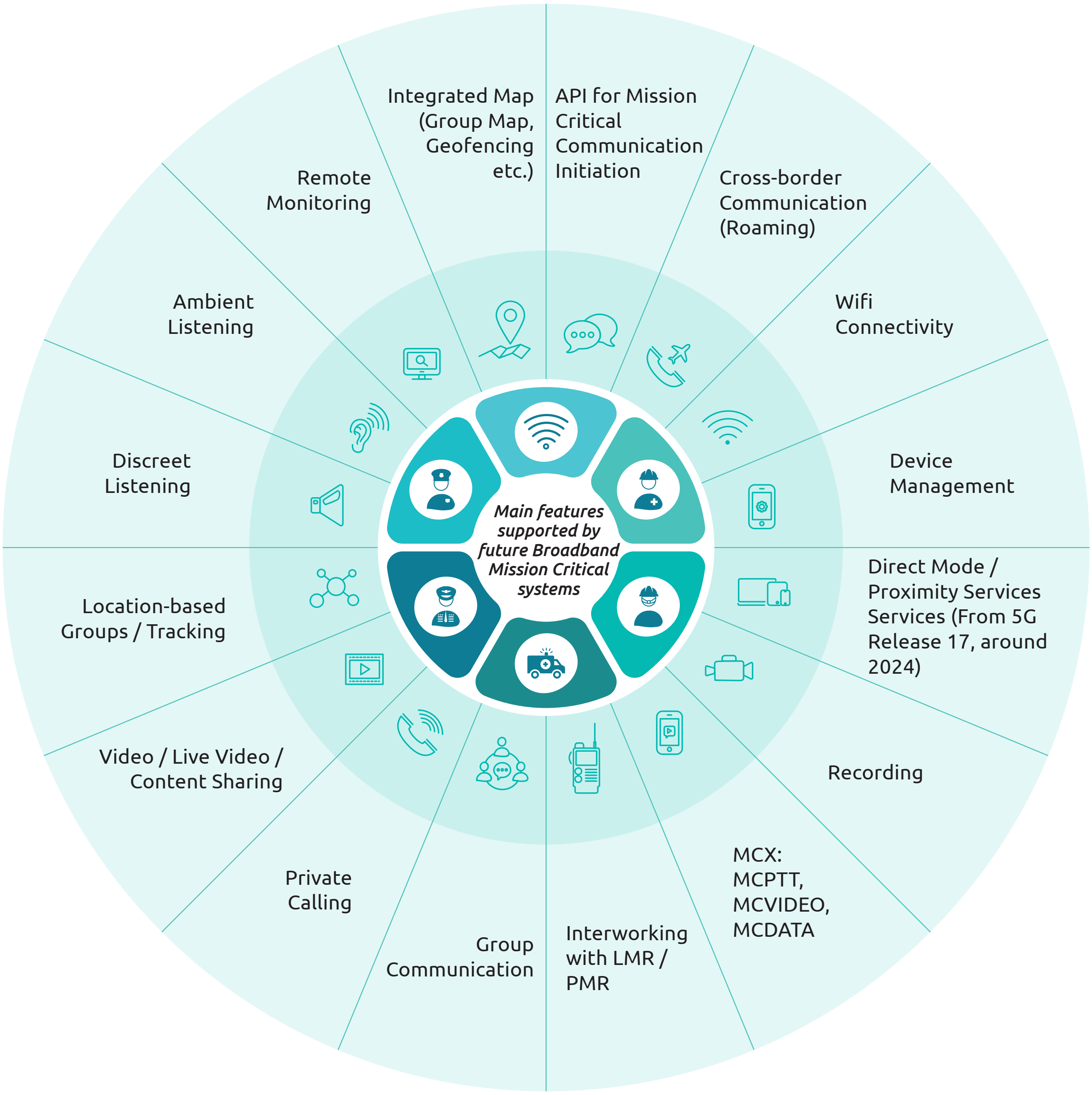
- **MCX integration on 5G architecture**
- **Direct Mode**
- **Broadcast**
- **...**

3GPP MCX features considered for 4G have been integrated for 5G (from R15 5G onward). All MCX features are being introduced, standardized, improved (e.g., adding Direct Mode & eMBMS in Release 17), and universalized (available to a broader audience) on the new 5G architecture.

[1] https://www.marketsandmarkets.com/Market-Reports/critical-communication-market-95862445.html; https://www.globenewswire.com/news-release/2021/06/15/2247673/0/en/Mission-Critical-Communication-MCX-Marketl

[2] https://www.globenewswire.com/news-release/2021/07/19/2264923/0/en/Global-Public-Safety-LTE-Market-

Mobile broadband solutions create new possibilities


Integrated Map (Group Map, Geofencing etc.)
API for Mission Critical Communication Initiation
Cross-border Communication (Roaming)
Wifi Connectivity
Device Management
Direct Mode / Proximity Services Services (From 5G Release 17, around 2024)
Recording
MCX: MCPTT, MCVIDEO, MCDATA
Interworking with LMR / PMR
Group Communication
Private Calling
Video / Live Video / Content Sharing
Location-based Groups / Tracking
Discreet Listening
Ambient Listening
Remote Monitoring
Main features supported by future Broadband Mission Critical systems

Technological evolutions have enabled new possibilities, thereby fundamentally changing the way things operate. The exchange of video- and data-based content will become the future standard. We foresee a mixture of voice and data-/video-based applications in multiple use cases during interventions. Broadband Mission Critical systems will be interconnected to Broadband mobile devices, but also to NB-IoT/LTE-M IoT devices such as cameras, drones, sensors, etc.

Every 3GPP release comes with a set of improvements and additional features (as aforementioned, those are the main features that will be supported by Broadband Mission Critical systems), that will enable new use cases (below are non-exhaustive examples for each of the main user groups). For broadband systems to become fully operational as a standalone solution, the main prerequisite is that all the capabilities and features of current LMR/PMR systems are supported to ensure continuity of services.

POLICE FORCES

- Dashcams & bodycams live streaming
- Biometric sensors and location
- Predictive threats & risks assessment
- Smart city monitoring
- Real-time location of field agents

FIREFIGHTERS

- Connected headset
- Hardened tablet and smartphone
- Drone (autonomous)
- 3D map and indoor location
- Live streaming intervention

MEDICAL & AMBULANCE SERVICES

- Connected ambulance with hospital video call
- Patient-vital sensors
- Bodycam – violence protection
- Remote surgery support
- Mobile access to patient data

OTHERS (DEFENCE, CUSTOMS, ETC.)

- Officer with connected equipment
- Tactical information sharing
- Automated admin reporting
- Maintenance and predictive logistics
- Remote office

Improving operational efficiency, productivity, and overall safety

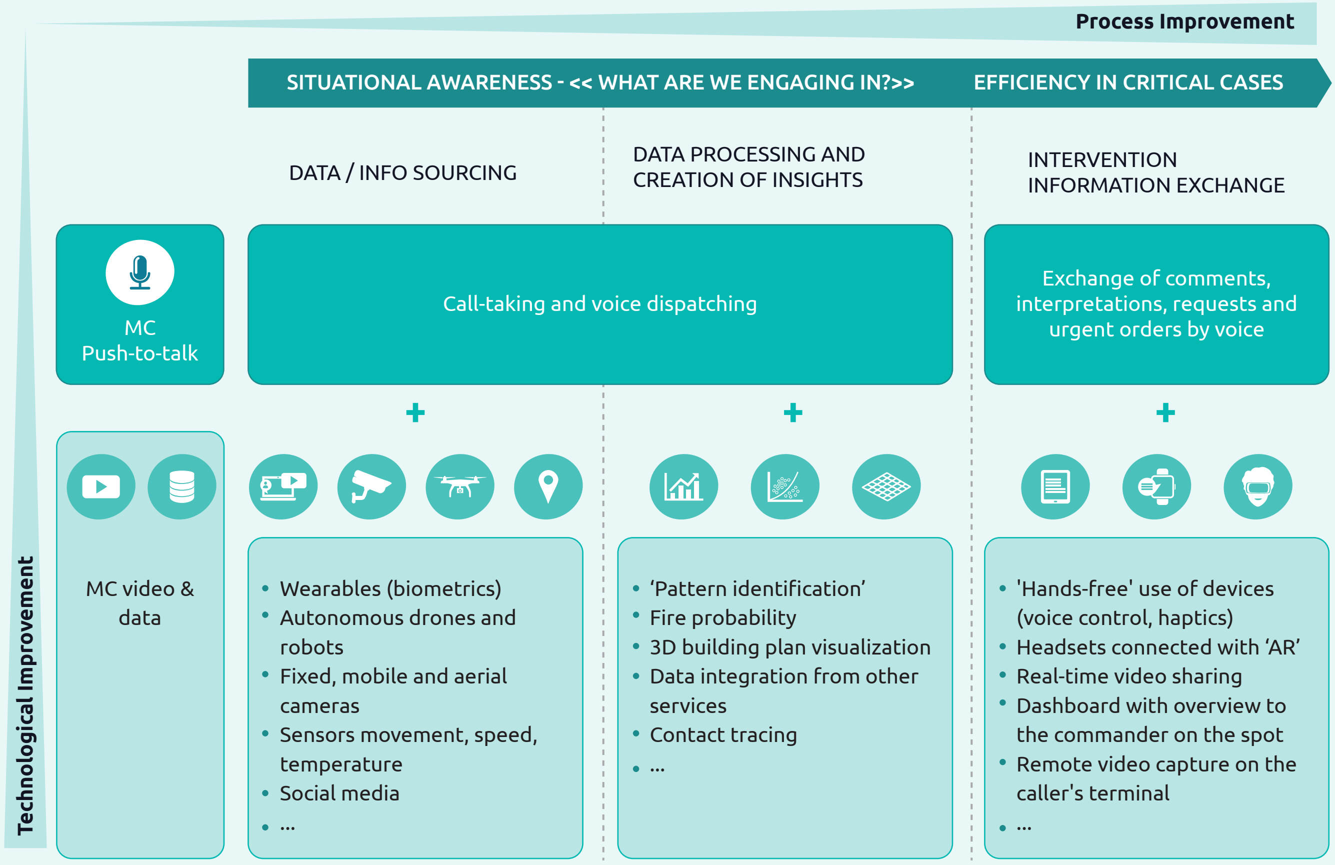
The technological evolution will impact the whole intervention value chain involving not only the Public Safety disciplines, but also the public and the call-taking/dispatching centers (PSAP).

Improvement will come in various ways; the combination of a high-performing network and data analysis via edge computing will allow for a more efficient management of interventions through the creation of a "Situational Awareness[1]," richer in context and insights. Legacy voice services used during intervention (Push-To-Talk, taking a call and voice dispatching) will be complemented with data transmission from multiple sources (e.g., sensors, IoT, cameras, social networks, etc.) and processing, first at dispatching centers, then directly on the field through smartphones, tablets, and other accessories. In other words, rescue and security services will be able to:

(i) Act proactively instead of only being able to react in the face of an ongoing situation;

(ii) Carry out interventions with enhanced situational awareness on the ground (even before taking any actions) and thus be better prepared.

These efficiency improvements will increase the safety of all.



Process Improvement

SITUATIONAL AWARENESS - << WHAT ARE WE ENGAGING IN?>>

EFFICIENCY IN CRITICAL CASES

DATA / INFO SOURCING

DATA PROCESSING AND CREATION OF INSIGHTS

INTERVENTION INFORMATION EXCHANGE

MC Push-to-talk

Call-taking and voice dispatching

Exchange of comments, interpretations, requests and urgent orders by voice

+

+

+

MC video & data

- Wearables (biometrics)
- Autonomous drones and robots
- Fixed, mobile and aerial cameras
- Sensors movement, speed, temperature
- Social media
- ...

- 'Pattern identification'
- Fire probability
- 3D building plan visualization
- Data integration from other services
- Contact tracing
- ...

- 'Hands-free' use of devices (voice control, haptics)
- Headsets connected with 'AR'
- Real-time video sharing
- Dashboard with overview to the commander on the spot
- Remote video capture on the caller's terminal
- ...

Technological Improvement

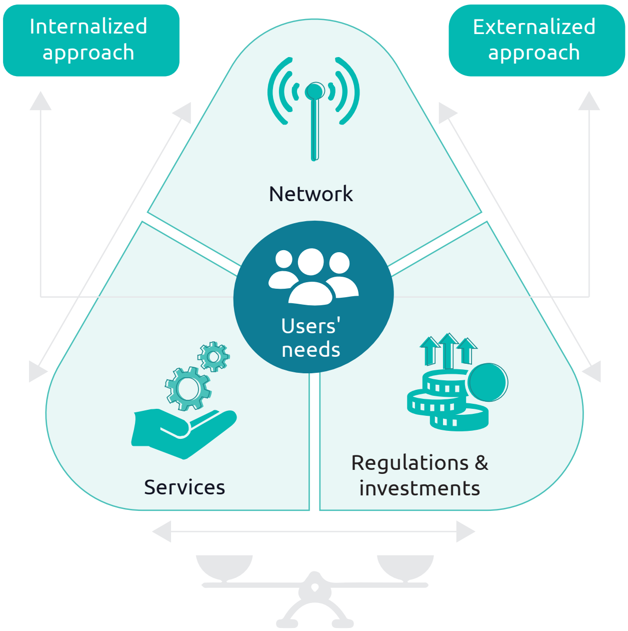
Legend: 🟩 *Current / Legacy Intervention process* ▢ *Future add-ons to the intervention process*

[1] The term "Situational Awareness" refers to the perception of elements and events surrounding a certain situation, time, and location.

New business models will lead to an optimized cost structure

The roll-out, maintenance, and operations of Public Safety networks are expensive. The shift towards Broadband systems creates a momentum for governments to rethink, and possibly adapt, business models (incl. systems ownership) and operations to optimize costs and thus increase budgetary control. Cost-related benefits stemming from the implementation of broadband services are a combination of multiple factors, namely improved productivity and efficiency, mutualized investments, collaboration at national and possibly international levels as well as leveraging existing commercial infrastructures and expertise, to cite a few relevant examples. New business models can be implemented as well, where important initial CAPEX investments could be replaced by OPEX, allowing more flexibility and agility (in terms of contracts, partners, solutions swapping, etc.). The benefits of future solutions must be assessed in light of resources available (financial and expertise), quality of service, existing assets and the priority of public service above all.

Finding the right balance to fulfill the users' needs



Organizing and implementing Broadband Mission Critical mobile broadband systems comes with a set of important requirements to be considered. At the heart of these requirements are the user needs and the mission of public safety and security to be fulfilled. These requirements can be classified into three main categories: Network, Services, and Regulations & investments.

> *"There are no real issues to build a MC mobile broadband network, but there are a few limitations such as ensuring feature standardization, coverage, and hardening."*
>
> ***– FirstNet, USA***

Network: The 3GPP standards are the basis of the Mission Critical 4G/5G mobile networks to ensure the highest QoS and interoperability. In addition, the network resilience and availability require specific hardening, extended coverage, preemption and prioritization mechanisms, and a prime focus on security.

Services: Continuity of services needs to be guaranteed, combined with a future-proof approach by foreseeing an open system allowing scalability and avoiding vendor lock-in. This is also applicable to all the devices, features, tools, and accessories used by each discipline. In addition, standardization is a must to ensure interoperability and compatibility of the solutions (incl. devices). Service security and confidentiality need to be a priority. A key success factor of the future services is a fully integrated end-to-end approach in the Public Safety value chain (e.g., dispatch integration).

Regulations & investments: The capabilities and set-up of the future Mission Critical systems will strongly depend on the regulatory framework availability of dedicated PPDR spectrum, MC obligations imposed on public network operators (prioritization & preemption mechanisms, etc.). In addition, setting-up a new communication system will require important investments. Governments must allocate sufficient budgets to the most critical components.

“The evolution toward broadband solutions must come with a set of appropriate legislations, enforced well in advance to make sure all stakeholders are aligned with the right regulatory framework and guidelines.”

– VIRVE, Finland

KEY TAKEAWAY:

Sooner or later, every country around the world will make the shift towards future Mission Critical communication systems. This will require some important decisions. It is not merely a matter of providing broadband connectivity, it also requires access to the right systems and tools that comply with Mission Critical requirements to guarantee the Public Safety mission. The challenge for governments is to find the right balance between network, services, and regulations, and investment requirements. This also requires defining the appropriate organizational, operational, and technical models of the future.

TOWARDS A FUTURE-PROOF MISSION CRITICAL ECOSYSTEM

The development of broadband Mission Critical systems is more than a choice of technology, it implies important organizational, operational, and technical considerations. Historically, Public Safety networks and organizations have often been decentralized, sometimes by geographic area or discipline. Gradually, the need for inter and intra disciplinary collaboration and interoperability became essential, pushing most governments to put in place a dedicated organization and systems. The shift toward the 3GPP ecosystem opens up new opportunities for telecom providers, questioning the relevance of such dedicated organizations and systems. In fact, who in the future, should be accountable and responsible to guarantee the best services and connectivity? Could mobile network operators (MNOs) provide better solutions, and thus replace dedicated Public Safety agencies? Operationally, who should manage and operate the Mission Critical systems and what should be the technical approach? To answer these questions, governments must be aware of the challenges ahead and take into account several key considerations.

Public Safety authorities will face many challenges and opportunities

Market Fragmentation

Business Critical and/or Mission Critical applications are converging towards the same 3GPP-based technologies. This opens up new opportunities to actors such as MNOs, private network suppliers, equipment vendors, etc.

Budgeting

Public Safety authorities must ensure sufficient budgets to build and operate the Mission Critical network components while ensuring cost effectiveness and financial viability of the new network.

Ecosystem Orchestration

Building and operating Mission Critical communication systems require the orchestration of a large ecosystem of partners. An end-to-end vision of the network & services is necessary to guarantee performance and flexibility, and avoid lock-in.

Technology

Public Safety authorities will have to ensure that the networks are future-proof and designed for maximum performance, resilience, reliability, security, interoperability, and evolutivity.

Discipline & User Adoption

End-users – from command centers to first responders, across all disciplines – must be at the heart of the transformation journey, from the design of systems, services, and operational processes to appropriate trainings and change management.

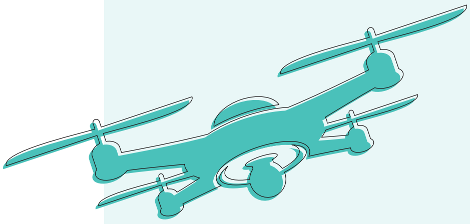
Migration & Timing

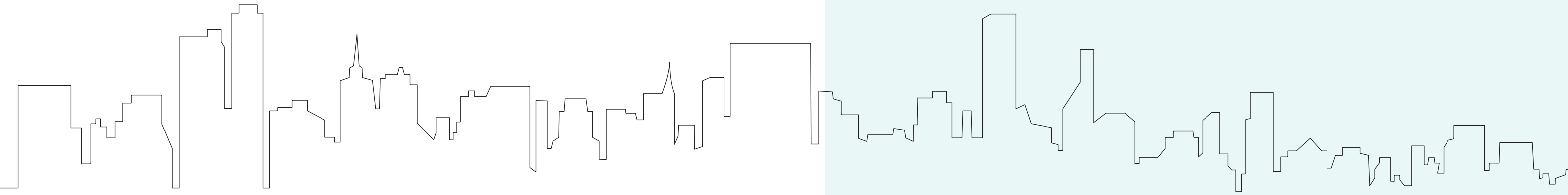
Designing, rolling out, and testing a new end-to-end Mission Critical communication system takes several years. In addition, migrating all disciplines to new devices, services, and processes requires careful planning.

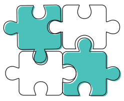
> *“Engaging the users before, during, and after the system deployment process and operations as well as having them closely involved in shaping the reinvestments and evolutions of the network is critical.”*
>
> ***– FirstNet, USA***

> *“We must remain pragmatic and in the first phase focus on the roll-out and implementation of a broadband network, and in the second phase add services and functionalities to comply with Mission Critical requirements.”*
>
> ***– VIRVE, Finland***

> *“For organizations driven by needs of vast number of commercial users vs. small numbers of Public Safety users and initiatives, things would always lean towards what the commercial user needs are as opposed to what the Public Safety needs are.”*
>
> ***– FirstNet, USA***







1. Market fragmentation

The fragmentation of the Mission Critical communication ecosystem is a real risk. Commercial, Business Critical, and Mission Critical applications will all be supported by the same technologies. This opens up new opportunities for actors such as MNOs, private network suppliers, equipment vendors, etc. to provide critical solutions. However, how can governments ensure the highest levels of confidentiality, security, and services interoperability to their users if multiple third parties are involved, specifically when solutions may target profitability over public interest?

As each discipline will have many possibilities available to suit their needs, global/nationwide considerations may be overlooked. In this case, interoperability issues between different solutions will appear, hampering the efficiency of operations. Inequalities between the solutions available to users in different locations will arise, in an environment where universality of services is key to ensure collaboration and interoperability.

2. Ecosystem orchestration

The support of commercial, industrial, and Public Safety applications on the same technologies will drive an ecosystem of solutions: network equipment providers, MCX service providers, device OEMs, mobile network operators, and system integrators. We foresee that the future Broadband Mission Critical ecosystem will drive partnerships to provide end-to-end solutions. This extended ecosystem can be an opportunity for Public Safety authorities to avoid long-term vendor/partner lock-in as it has been the case in some countries with legacy solutions.

3. Budgeting

Most investments for the current systems were done in the development and roll-out phases. Operating costs are generally quite high as the supplier ecosystem is limited, allowing little to no competition. On the contrary, as the Broadband MC environment increasingly involves a bigger diversity of actors, it should drive costs downward.

The future MC ecosystem will provide new possibilities in terms of organizational, operating, and technical models including potential partnerships with private/commercial actors, allowing to leverage synergies. Although, overall networks and running costs may be lowered, government must ensure sufficient budget to provide appropriate equipment on all critical components of the future network, while finding the right balance to guarantee long-term financial sustainability of the services.

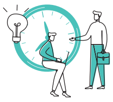
4. Technology

The standardization of broadband services is under development, implying that the technology is not yet mature enough to support all the Mission Critical requirements and applications (e.g., device-to-device communications). Public Safety authorities will have to ensure that the networks used are robust and future-proof. This implies supporting and accommodating technology evolutions, new solutions (applications, tools, devices, etc.), and being able to interconnect in broader ecosystems (i.e., internationally).

Data & information management is a challenge as well. In fact, broadband technologies also imply that the influx of information and data coming from multiple and various sources will drastically increase. This can improve process & intervention efficiency and collaboration, only if all these new sources of information are well-integrated with each other and available to all relevant users to increase situational awareness.

5. Discipline & User Adoption

Public Safety users and agencies are generally attached to their communication tools and solutions. As such, authorities will most likely be challenged by the users on the need to evolve or on the way to evolve. The first challenge will be to align and convince users, not only from the same groups but also between groups (e.g., police forces and firefighters, etc.). Change management campaigns will be needed to gain consensus and buy-in from all users in various geographic areas to ensure a seamless evolution. Involvement of all disciplines and users in the migration process (from the development phase to actual roll-out) is a key success factor.



6. Migration & timing

Timing is essential for a smooth transition towards new technologies. Designing, rolling out, and testing a new MC network takes several years. The challenge is to make sure that authorities act without delay to start the transformation journey to plan system and device migration, and technological evolutions, but also secure trust from users, and international integration on a broader ecosystem.

A central and dedicated agency will guarantee the integrity of the systems

A central and dedicated Public Safety organization can play different roles in network operations. Some countries may opt for an approach in which the Public Safety organization ensures the overall management and coordination, while the actual roll-out and servicing is outsourced to commercial parties such as MNOs. Other countries may prefer that their Public Service organization directly reports to the government and is responsible for the end-to-end management of Mission Critical communications. The specific characteristics of organizational models in each country will differ depending on the maturity and state of the MC ecosystem, but a central and dedicated Public Safety organization, seems best suited to fulfill all requirements for several aspects:

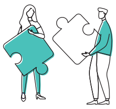
1. Sovereignty over the national Mission Critical communication services

In the Mission Critical ecosystem, the purpose and nature of Public Service should always prevail. Governments will have to mobilize means and resources to ensure supervision (i.e., administrative, organizational or technical, etc.) of any private subcontractor. This can be done via a central and dedicated organization, a trusted partner with a dedicated mission, focusing on public services only, offering greater organizational and operational flexibility, dedicated services, and customization with a proactive focus on the users. In fact, Public Safety disciplines have sometimes different, sometimes similar needs in terms of communications. This means that the solutions they are using must best fit their specific need fulfilling a common basis of requirements in a fully integrated and interoperable system. A central, dedicated, service-based organization that is “user/discipline-oriented“ can provide the architecture needed to ensure that there is flexibility and agility to implement and/or integrate dedicated functions and features for Public Safety applications. Such organization/agency is best positioned to understand and anticipate (i.e., technology watch) the needs of all first responders, but also make sure that the relevant solutions are provided – in other words, a Public Safety organization and system developed for Public Safety disciplines in close collaboration with the disciplines themselves.

Ensuring the public’s best interests also means making the most relevant choices in terms of technologies, devices & accessories, evolution roadmap, overall investments, dedicated spectrum etc. without commercial interests. A dedicated organization with sovereignty over the communication systems, and control over the budget and resources, can take decisions best aligned to the Public Safety mission in the long run, thereby driving innovation forward.

> *“A dedicated organization provides a guarantee of service while putting public needs and interests as a priority, not profits.”*
>
> ***– FirstNet, USA***

> *“A central and dedicated organization is the only way government can guarantee that the public’s best interests are put above all things.”*
>
> ***– ASTRID, Belgium***



2. A central, common, and unifying approach

The evolution towards broadband systems is an opportunity to ensure universality of services. Broadband MC applications can enable more collaboration within and between disciplines. A central and dedicated organization, serving all disciplines, with common systems and approach is best positioned to foster technical and operational interoperability, avoid silos, thereby benefiting all users, and act as a common voice towards suppliers and partners.

> *“We chose to go for a centralized approach to provide common guidelines to all disciplines on a national level through a central and dedicated organization.”*
>
> ***– VIRVE, Finland***

3. Be the SPOC for all users

When users need support, a simple and central point of contact, responsible and accountable for all communication affairs is needed.

A SPOC is also important on an international level. International collaboration has become a relevant topic in the last decade when crises such as terrorist attacks have highlighted interoperability issues. Since broadband solutions are easily interoperable, countries will have the ability to exchange voice, data, and video with each other (the EU Broadway initiative is a concrete example).

> *"A central and dedicated organization acts as a SPOC and intermediary between all stakeholders involved for all matters associated with Public Safety communications."*
>
> ***– VIRVE, Finland***

A single organization managing Public Safety communications is best suited to organize international collaboration (cross-border collaboration, Standardization bodies like ETSI, GSMA, 3GPP, etc.). The European Broadway initiative is a concrete example of international collaboration between dedicated Public Safety organizations to build a "borderless" broadband Mission Critical network.

4. Ensuring inter and intra disciplinary support without discrimination

Although having the same fundamental mission, each discipline has specific needs in terms of usage and context and thus also in terms of communication requirements. For example, while police forces use their communication tools for day-to-day operations (e.g., file building, mobile office, etc.), fire brigade and ambulance services need theirs for coordination and situational awareness mostly in ad-hoc emergency situations. On a national level, disciplines should be aligned to find a common ground of features to implement on a Broadband MC network. This is only possible if an independent actor communicates, listens, and federates users without making differentiation to make sure that there is as much mutualization or common ground as possible, with flexibility to implement additional specificities.

A central and dedicated agency focusing on Public Safety users has the advantage to be best positioned to fully understand the users' operations and thus translate needs, requirements, and concerns into relevant solutions.

> *"The proximity with the users is crucial to develop the appropriate solutions."*
>
> ***– ASTRID, Belgium***

> *"Before setting up our nationwide network, we did a tremendous amount of outreach to the users to find out what they wanted based on their needs."*
>
> ***– FirstNet, USA***

5. Ensure seamless integration of the whole intervention process

Public Safety communications need to consider the complete value chain of the intervention process and all associated tools need to be addressed. From the general public's resources to reach out to Public Safety organizations to the call & dispatch centers (PSAP) coordinating all interventions up to the MC systems used in actual operations, all need to be factored in. A centralized oversight on all these components is needed to ensure end-to-end integration of communication and data management.

> *"An optimal service delivery requires the end-to-end integration of infrastructure underpinning the whole intervention process."*
>
> ***– ASTRID, Belgium***

6. Be the safeguard of security, confidentiality, and authenticity of traffic and data

Special attention needs to be given to the security of data and communication flows. As a large part of the MC communications involve private, confidential and/or sensitive information, security is a key prerequisite. To mitigate internal and external risks, robust cybersecurity mechanisms should be implemented, in addition to limiting, but also controlling, the number of actors intervening, as much as possible. At the same time, all relevant information needs to be available on the spot for all relevant users.

> *"The expectation from the government is to have the guarantee of security for customer data and user map information transiting in the network."*
>
> ***– SWISSCOM, Switzerland***

KEY TAKEAWAY:

To manage all Public Safety related communications, a trusted central and dedicated organization is best placed to ensure safe and reliable information exchange. Multiple aspects and components within the value chain must be integrated and aligned. To ensure the public interest, decision makers need to set-up an overall oversight to monitor the MC network system, its changes and evolutions, and to make fast decisions aligned to the public interest as a top priority.

A common, central, and dedicated Mission Critical network

In several countries, cities and/or disciplines have set up their own private and customized broadband solutions to take advantage of mobile video and data exchange. This may present opportunities in the short term in terms of time-to-market (decision making, network and services roll-out). However, in the long run there will be disadvantages.

> *“The need for collaboration and interoperability issues associated with multiple decentralized initiatives pleads for the establishment of a central national network.”*
>
> ***– ASTRID, Belgium***

> *“Government will conclude that all cantons must have the same system nationwide with a centralized approach.”*
>
> ***– SWISSCOM, Switzerland***

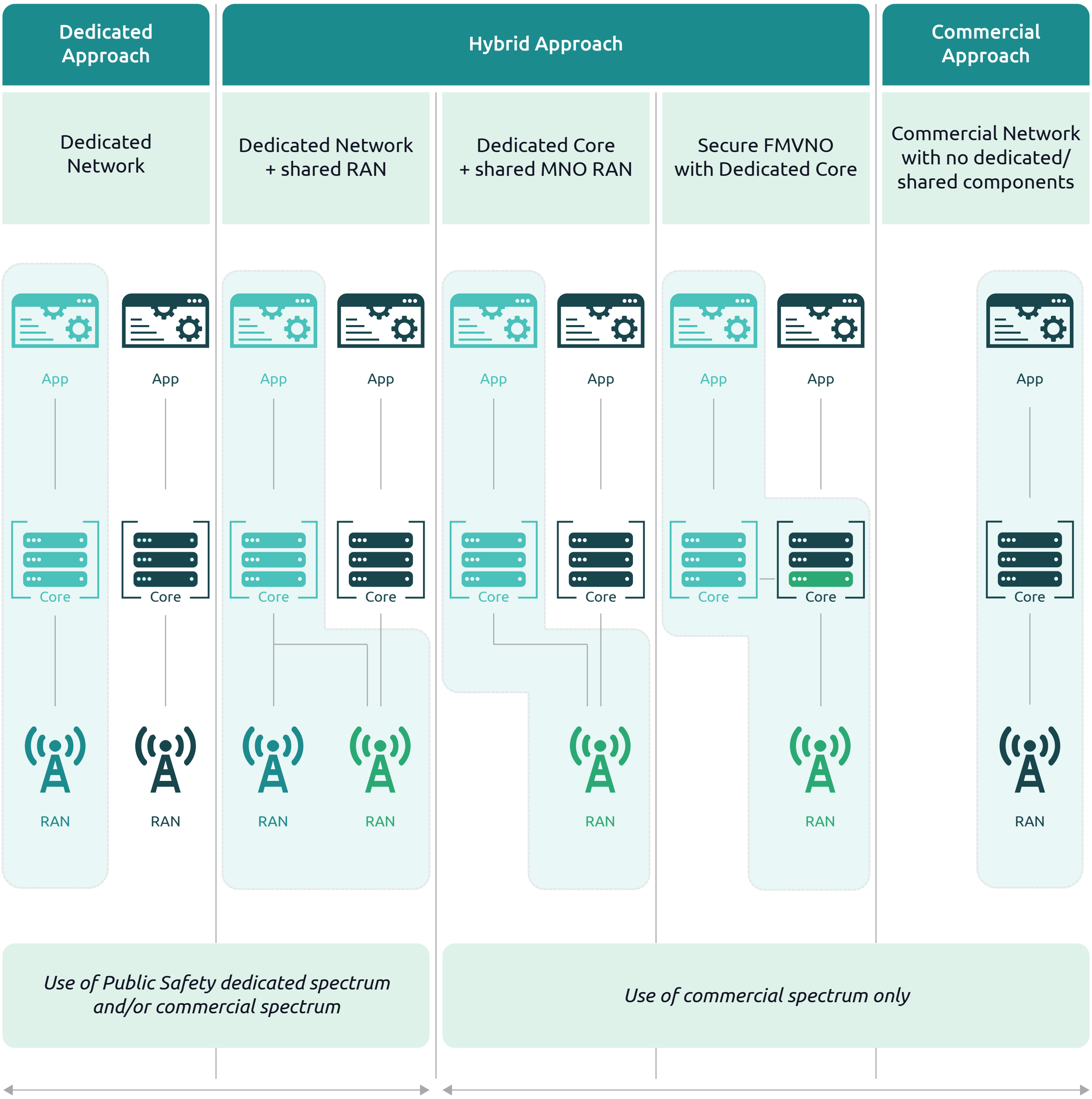
In an ecosystem where collaboration, interoperability and universality of services are key requirements, a decentralized approach creates more potential points of failure and increases technical complexity. Moreover, local initiatives are reserved for the “happy few”, causing other users in less populated areas or with less resources to be excluded. Interoperability between multiple decentralized networks based on seamless integration is, and will also be in the future, a major technical challenge. Partial interoperability can be reasonably considered under specific conditions (i.e., extending the central network in remote and uncovered locations) but remains a workaround.

> *“The implementation of a nationwide network has been a game changer for interoperability.”*
>
> ***– VIRVE, Finland***

The multiplicity of networks can be expected to be more expensive. Multiple initiatives and networks in the same country may lead to duplication of resources and effort. The fragmented organizations will have to negotiate without benefiting from the economies of scale and negotiation power of a central, larger organization. This economic disadvantage is applicable on network elements but also for devices and development of specific tools.

While longer to implement, a national approach to providing Mission Critical communications across disciplines, with in-depth knowledge of their operations and with the required network assurance and quality of services, draws significant technical and budgetary advantages.

Combining commercial and dedicated assets to leverage the best of both worlds



Dedicated Approach	Hybrid Approach			Commercial Approach
Dedicated Network	Dedicated Network + shared RAN	Dedicated Core + shared MNO RAN	Secure FMVNO with Dedicated Core	Commercial Network with no dedicated/ shared components

Use of Public Safety dedicated spectrum and/or commercial spectrum

Use of commercial spectrum only

Legend :

- ■ Operator / MNO assets
- ■ Public Safety Operator assets
- ■ Shared assets (MOCN / MORAN)
- □ Public Safety Network components
- App: MCX, VoLTE, etc.

Next to the choice on how to organize Mission Critical communications, a choice needs to be made on the network architecture and operating model. Several models are possible for the implementation of broadband services for Public Safety depending on each country's situation and ambitions.

Broadband MC systems can be implemented with a dedicated approach, i.e., an end-to-end MC communications network separated from commercial 4G/5G public networks. This set-up has been implemented in several countries; South Korea's Safe-Net is one example. Other countries have chosen an approach largely relying on commercial networks, such as the United Kingdom with the Emergency Services Network (ESN) project from Home Office, or the United States with FirstNet. Such an approach makes sense as rolling out a fully private/dedicated Broadband MC network is generally far above the financial resources and/or willingness of most governments. However, in practice, relying on a commercial network to ensure Mission Critical services still requires additional investments to upgrade the public network to the level of performance, reliability, and security required for Mission Critical communications. This investment will include coverage enhancements, equipment hardening, prioritization mechanisms, etc.

Another approach that combines the best of both worlds is the hybrid model in which both dedicated and commercial resources are pooled and combined to build a customized system. This means leveraging the strengths and existing assets of commercial operators – the radio network coverage, in particular. In addition, dedicated infrastructure and features (coverage extensions, back-up solutions, hardening, MC features, prioritization mechanisms, usage of dedicated PPDR spectrum, etc.) can be added. Such a model ensures that all MC and Public Safety requirements are guaranteed, but also that users benefit from the latest innovations brought by the commercial market, while assuring confidentiality and being in full control of MC aspects like priority, preemption, etc.

> *"It requires so much time, investment, and negotiation power to build a totally new dedicated network from scratch. it is almost impossible to do it cost effectively without the synergies commercial actors can provide."*
>
> ***– FirstNet, USA***

> *"A hybrid model in which the best capabilities and assets from public and commercial actors are combined is the most appropriate approach."*
>
> ***– ASTRID, Belgium***

> *"With a dedicated approach, everything MNOs must do to become Mission Critical would need to be done as well. Starting from scratch would imply much more investments than leveraging existing assets and synergies."*
>
> ***– SWISSCOM, Switzerland***

Based on local specificities, ambition, and resources available, Public Safety authorities must determine the appropriate network strategy, considering the Mission Critical aspects. The latter should be managed and operated by a trusted actor, preferably the Public Safety authorities themselves. Overall, past experience and case studies agree on the imperative need of a dedicated broadband core network[1], supporting all needed MC features and requirements to ensure control, availability, and safety of the traffic and solutions (incl. data privacy). A dedicated core network operated by a trusted actor, in combination with a tailor-made public radio network[2] guarantees Mission Critical communications such as preemption and prioritization of users and data flows at any time.

> *"We believe that managing and operating a dedicated core network is a necessity for any Public Safety network, simply to ensure universality of services and interoperability."*
>
> ***– VIRVE, Finland***

> *"Ensuring preemption of users is important, but in a Mission Critical environment, not all data flows and usage need to have the same level of priority."*
>
> ***– ASTRID, Belgium***

[1] Multiple network architectures are possible (i.e., FMVNO, MOCN, MORAN, see figure on previous page). One common component is the separation of Core vs. RAN activities and equipment, the former being one of, if not the most critical component.

[2] This means commercial RAN infrastructures possibly with dedicated PPDR spectrum

The time to act is now

The migration towards a new broadband network is a complex transformation journey. As continuity of service is a fundamental requirement, it is expected that both legacy narrowband and broadband Mission Critical systems will coexist for some time because the full development and implementation of the latter solutions will take several years. The question remains, however, when should Public Safety authorities start the deployment of broadband solutions?

> *"Our approach is dependent on our own country-specific parameters, there is probably no one size fits all."*
>
> ***– VIRVE, Finland***

The time to start is determined by user needs. Mobile broadband solutions can be started quickly but will probably not yet support all the features and capabilities of current LMR/PMR systems (e.g., direct mode). The MC ecosystem shift is a big challenge for the Public Safety community. In fact, migrating from narrowband to broadband solutions (incl. tools, devices, etc.) is complex, and will take time, requiring developments, trainings, and a learning period. As such, Public Safety authorities must define clear organizational, operational, and technical targets ahead of time to prepare and ensure a smooth migration. Delaying the transformation journey risks increasing the financial burden for governments, and thus the users themselves. Legacy and next-generation MC systems will be operated simultaneously, implying duplication of efforts and resources (human resources, investments, devices & accessories, etc.)

> *"We fully expect a parallel use of the FirstNet network and traditional LMR networks for an undetermined period before trust on broadband MC systems is established."*
>
> ***– FirstNet, USA***

> *"To ensure a smooth migration, it is crucial to involve all user organizations as early phase as possible in the migration process."*
>
> ***– Virve, Finland***

> *"Today, it is not realistic to have a Public Safety broadband network without legacy LMR systems running in parallel to ensure service continuity."*
>
> ***– ASTRID, Belgium***

> *"Interoperability between legacy solutions and future solutions is key in the migration of users."*
>
> ***– SWISSCOM, Switzerland***

Overall, it is best to quickly start the learning period and migrate proactively while gradually implementing new solutions and features. Reducing the time to migrate brings financial relief as legacy systems can be sooner taken out of service. Therefore, Public Safety authorities must proactively support users to facilitate the migration.

KEY TAKEAWAY:

A nationwide unified hybrid network combining one (or several) mobile public network's assets with dedicated Mission Critical network assets is balancing at best the Mission Critical requirements and the financial implications and complexity of rolling-out a new network from scratch. The commercial network can be upgraded where needed and be connected to dedicated network components that guarantee the required autonomy, reliability, and security. It can be complemented with deployable (portable solutions) that can guarantee communication when there are no connectivity means left.

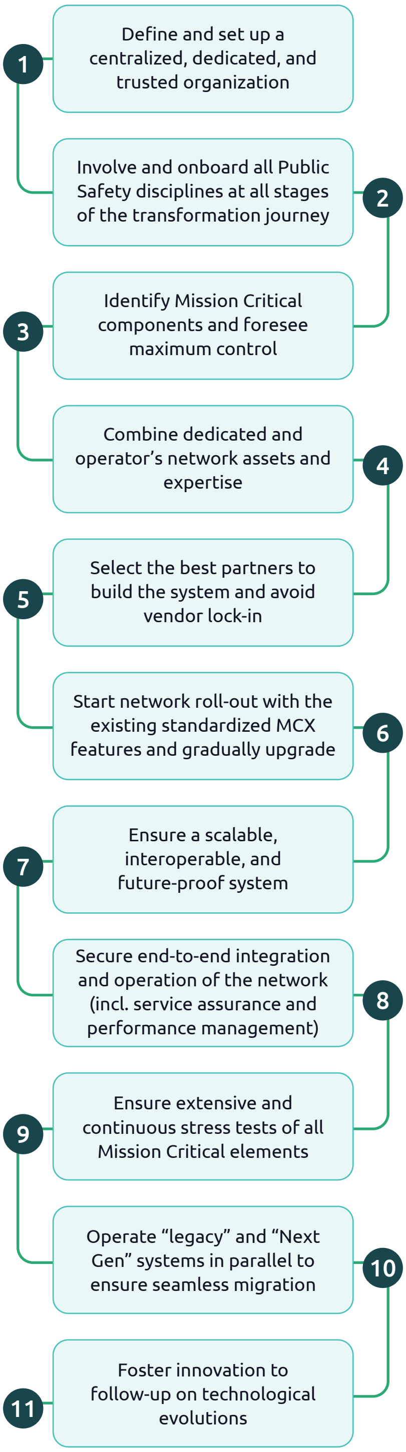
To maintain the integrity and neutrality of such a network, its supervision should be entrusted to a central and dedicated actor, a "trusted operator" with the sense of urgency and a culture of commitment for Public Safety and security, a more difficult aspect to implement within a commercial operator.

Setting-up and operating such a Mission Critical communications network and managing the actors in the ecosystem requires specific skills. Recruiting and upskilling talent will be another challenge for new organizations, but an absolute pre-requisite to building a strong and sustainable Public Safety player.

TRANSFORMATION OF PUBLIC SAFETY COMMUNICATIONS, A WORLDWIDE HOT TOPIC

Country	Highlights	Attributed PPDR Spectrum	Dedicated central agency	Broadband Operational model
Australia	• In 2019, the Australian government recognized the need for a PS Mobile Broadband network for its emergency services. • PoCs are being developed since **2018.**	✓	✓ National governance to set-up guidelines	**Commercial Model** It would appear the Australian government will rely on commercial network complemented with additional spectrum
Belgium	• Belgium has reviewed its PS communication strategy to roll-out a new Mobile Broadband MC network nationwide. • Implementation expected in **2023-2025.**	✓	✓ ASTRID – operator	**Hybrid Model (MOCN)** Dedicated Core network interconnected with operator and dedicated RAN. Network operated and hardened by ASTRID
Dubaï	• Dubai has created the "Nedaa" organization, a government secure network provider, dedicated to professional communications. • Broadband services provided to PS on LTE.	✓	✓ Nedaa – operator	**Dedicated Model** Dedicated Network (Core and RAN) set-up for PS disciplines and other safety and security actors
Finland	• Finland is currently developing VIRVE 2.0, the second generations of PS network based on LTE/5G technologies. • Implementation expected in **2023-2025.**	✗ May change in the future	✓ VIRVE – operator	**Hybrid Model (MOCN)** Dedicated Core network interconnected with operator and dedicated RAN. Network operated and hardened by VIRVE
France	• France is currently modernizing its Public Safety communication systems with a centralized approach supporting Broadband apps. • Implementation expected in **2022-2025.**	✓	✓ ACMOSS – operator	**Hybrid Model (FMVNO)** Dedicated Core network interconnected with the Core and RAN of two operators, and managed by a dedicated organization
Germany	• Germany currently operates a TETRA-based nationwide network to handle all PS communication needs. • PoCs are being tested but no official agenda is set to roll out a Broadband network.	✓	To be determined	To be determined
Netherlands	• The Netherlands operates a TETRA-based nationwide network (C2000) and plans to keep maintaining it for a while. • Mobile broadband solutions will be provided by commercial network operators.	✓	✗	**Commercial Model** Broadband services will be delivered by commercial operator, next to TETRA network
Singapore	• Singapore PS disciplines use a dedicated but private actor (grid communications) for their critical communications. • The provider has gradually evolved to offer data services to PS users.	✓	✗	**Commercial Model** Broadband solutions provided by a commercial player specialized in professional communication.
S. Korea	• South Korea has rolled-out the first mobile Broadband networks in the world for their PS, railroad, and maritime services. • The PS-LTE network is in full service **since 2018.**	✓	✓ Safe-Net – operator	**Hybrid Model (MOCN)** Dedicated Core operated by Safe-Net interconnected to the RAN of several operators
Switzerland	• Switzerland has a nationwide TETRA-based network (Polycom) but has issued RFP to develop mobile MS broadband solutions for PS. • Current broadband solutions are provided by public operators (non-critical solutions).	To be determined but most likely	To be determined	To be determined
UK	• The UK has started to develop a MC network for its PS agencies through a private actor that acquired the former TETRA network. • Several issues were encountered delaying the implementation **to 2024-2025.**	✗	✗	**Commercial Model** Broadband services will be delivered by commercial operator
USA	• The US have set up a dedicated agency (FirstNet) that partner with a national operator to roll out a nationwide LTE Network. • Network is running **since 2018** and keep improving with MC features and requirements.	✓	✓ FirstNet – supervision	**Hybrid Model (MOCN)** Dedicated Core network coupled with operator's RAN. Network fully managed by operator

ACTION PLAN TO TACKLE THE CHANGE



1 Define and set up a centralized, dedicated, and trusted organization

2 Involve and onboard all Public Safety disciplines at all stages of the transformation journey

3 Identify Mission Critical components and foresee maximum control

4 Combine dedicated and operator’s network assets and expertise

5 Select the best partners to build the system and avoid vendor lock-in

6 Start network roll-out with the existing standardized MCX features and gradually upgrade

7 Ensure a scalable, interoperable, and future-proof system

8 Secure end-to-end integration and operation of the network (incl. service assurance and performance management)

9 Ensure extensive and continuous stress tests of all Mission Critical elements

10 Operate “legacy” and “Next Gen” systems in parallel to ensure seamless migration

11 Foster innovation to follow-up on technological evolutions

Reliable mobile communication services are a real lifeline during interventions and emergency situations. This highlights the importance of tackling the change towards the 3GPP Mission Critical ecosystem with much attention and precautions. Although, most of the mobile broadband traffic can be conveyed over regular commercial mobile networks, the communication systems used by Public Safety disciplines require networks with a much higher degree of robustness and availability embedded with specific mechanisms and features to enforce prioritization and preemption of users and data flows. In the most critical cases (e.g., when lives are at risk), first responders need the guarantee that their communication systems and tools are available anytime, anywhere, and with the highest QoS.

One of the responsibilities of Public Safety organizations is to fulfill the specific and stringent requirements of their users. Relevant organizational, operational, and technical models must be put in place to enable a Mission Critical broadband support of voice, data, and video applications at all stages of the Public Safety value chain (from civilians in distress, to field agents, through call & dispatch centers). While some countries have embarked early upon that complex transition journey, most countries are at a turning point and are confronted with difficult choices.

Public Safety actors should be able to rely on a centralized and trusted organization that has in-depth know-how on the first responder’s operations and can translate the needs and concerns into technical requirements and solutions. Each country will have to identify the right balance between public interest, the needs of the users, the technical capabilities (network and services), and regulatory and financial constraints. Due to the lack of means and resources to roll out a fully dedicated and proprietary broadband system, the outcome of this exercise will, in most cases, be a hybrid approach, leveraging commercial assets and expertise mixed with dedicated Mission Critical infrastructure, equipment, and features. Public Safety authorities should avoid the multiplication of local and private solutions and network fragmentation as they form barriers to collaboration and interoperability that are detrimental to effective emergency services.

Migration between “legacy” and “Next Gen” systems will take place gradually; governments should expect that both systems will run in parallel for several years until broadband networks can fulfil all Mission Critical requirements (in terms of features and infrastructure) to become a standalone solution and allow a seamless migration. Considering the long implementation and migration process, now is the time to take action to prepare the Mission Critical networks of the future.

ABOUT THE AUTHORS

Pierre Fortier
Vice President – 5G Global Lead,
Capgemini Invent
pierre.fortier@capgemini.com

Patrice Crutel
Director – Technology & Platform Strategy,
Capgemini Invent
patrice.crutel@capgemini.com

Frédéric Vander Sande
Vice President – Telecom, Media & Technology Benelux,
Capgemini Invent
frederic.vandersande@capgemini.com

Olivier Gossart
Consultant – Strategy, Innovation & Design,
Capgemini Invent
olivier.gossart@capgemini.com

Stefaan Vyverman
Senior Manager – Benelux 5G Lead,
Capgemini Invent
stefaan.vyverman@capgemini.com

Industrial organizations are harnessing the power of data and digital to enhance operational performance, increase flexibility and agility, and unlock innovation and new business models. This digital acceleration brings connectivity challenges to center stage. To become more "intelligent," organizations need advanced solutions to collect, share, and process exponential volumes of data in real time, with the right scale, velocity, and security. New technologies like 5G offer key capability to fulfill these promises.

Capgemini Invent supports telecom operators and industry vertical players in unleashing the digital transformation potential. We add value by helping our clients envision, anticipate, and build on what new technologies bring to their business.

Capgemini Invent has acquired significant experience in the field of Mission Critical communications for Public Safety operators by supporting governments and agencies in their transformation journey towards mobile Mission Critical broadband communications. This experience combined with extensive research and interviews with experts and telecom operators has positioned Capgemini Invent at the forefront of this transformation.

Contact us for more information!

Capgemini invent

About
Capgemini Invent

As the digital innovation, design, and transformation brand of the Capgemini Group, Capgemini Invent enables CxOs to envision and shape the future of their businesses. Located in more than 36 offices and 37 creative studios around the world, it comprises a 10,000+ strong team of strategists, data scientists, product and experience designers, brand experts, and technologists who develop new digital services, products, experiences, and business models for sustainable growth.

Capgemini Invent is an integral part of Capgemini, a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of 270,000 team members in nearly 50 countries. With its strong 50-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fuelled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering, and platforms. The Group reported in 2020 global revenues of €16 billion.

Visit us at

www.capgemini.com

GET THE FUTURE
YOU WANT