Operators’ role in next generation MCX

Mission-Critical; Edge; 5G; PPDR; Business-model

White paper

Version 1.0, January 2021

Introduction

Governments and companies need their public protection and disaster relief (PPDR) teams and critical national infrastructure (CNI) to accurately evaluate an incident and its context, ensuring the right means and actions are involved, with high operational efficiency and providing the best timely response. Current narrowband technologies used by emergency services are a trusted way to transmit voice. Still, they cannot meet the requirements for the integration of new communication components, such as video, telemetry, remote monitoring and control, required for real-time scenario analytics. These Services must be available even in extreme circumstances, guaranteeing that rescue organizations can effectively collaborate when dispatching and managing heterogeneous intervention teams.

The quest for efficiency, security, and prediction is changing the paradigm of information collection and dissemination by PPDR organizations, which no longer depend only on mission-critical communications but are starting using mission-critical intelligence [1], defining the requirements for the next generation mission-critical communications.

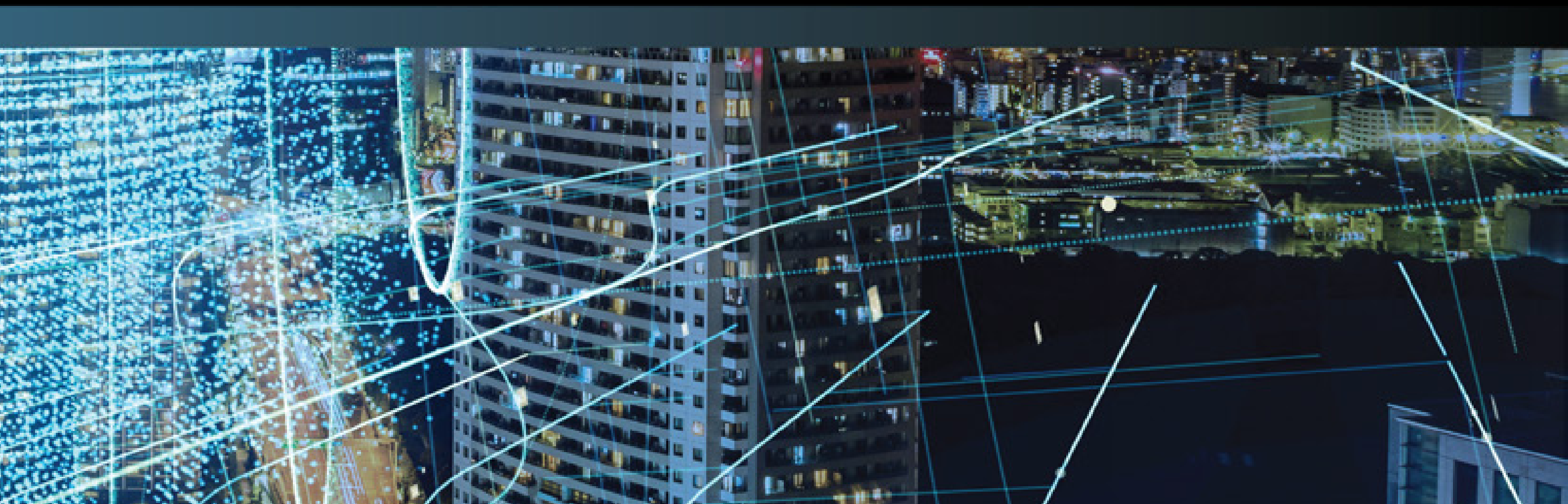
The need for a new approach, based on operators’ infrastructures, is generally accepted and already reflected by entities such as the European Commission, which already concluded in a 2014 study that “*commercial mobile broadband networks could be used for mission-critical communications with the right legal, regulatory and contractual framework and only if several requirements are fulfilled*.” [2]

In this context, 5G networks are emerging as being capable of supporting those new services, with the required availability and reliability, as well as enabling the functional vectors of next generation mission-critical intelligence, connecting everything everywhere, and providing contextual awareness, intelligent ecosystems, and critical intelligence.

Thus, 5G is the next big step, with efficient implementations and better answering requirements of coverage, availability, and security, at an affordable cost.

Next generation mission-critical communications enable PPDR actors to use the 5G broadband wireless network in use cases that will allow them to create a situational and contextual awareness within the geographical perimeter of the crisis scenarios. Use cases with great relevance are the following:

- **Video-surveillance for disaster relief:** the use of surveillance drones to aid the problem of tracking humans quickly from a distance in areas with difficult or slow access, or unsafe for a human to reach;
- **Remote diagnostics in a connected ambulance:** the use of augmented reality, virtual reality, and robotics in an ambulance to allow clinicians to assess and diagnose a patient remotely, view medical records, vital signs, and ultrasounds;
- **Robotic remote operation:** the use of remote-controlled robots to enable specialized people avoiding the risks associated with performing specific tasks at places of difficult access or with dangerous working conditions;
- **Real-time remote health monitoring:** the transmission of physiological signals, collected from wearable or implantable medical devices, from PPDR actors operating in crisis scenarios.



Technological components: 5G and the edge

In the context of mission-critical services (MCX), 5G, as seen before, is surrounded by expectancy and has the potential to play a relevant role. In a shared environment, edge computing is the perfect 5G companion to exploit its characteristics and guarantee the required reliability levels at reduced costs.

5G

5G is observing a widespread deployment, based on 3GPP Rel-15 (5G Phase 1) specifications and the defined non-standalone (NSA) mode of operation, adding additional bandwidth to existing 4G networks. 5G deployments in standalone (SA) mode (requiring a 5G Core), based in the same Rel-15, started by middle 2020, with a first related announcement made by T-Mobile in August 2020 [3].

In past July, the first set of 5G Phase 2 standards were approved [4], providing all required features to support 5G enhanced mobile broadband (eMBB), massive machine-type communications (MTC), and ultra-reliable and low-latency communications (URLLC) use cases [5]. Only at this stage is 5G accomplishing its main objective of answering B2B communications' requirements, like reliability and low latency, besides improving targeted B2C services (e.g., with more bandwidth and higher moving speeds). In that context, several verticals will be able to exploit a shared 5G infrastructure via tailored slices to their needs, with slicing being explicitly and natively supported as its edge computing. 5G incorporates the native capacity to provide access to services from the core, to the very near edge, possibly from service platforms located at or very close to cell sites.

MCX, where the public protection and disaster recovery (PPDR) area fits, will benefit enormously from exploiting common 5G features, like general lower latency, improved resilience, and accurate localization information (Rel-16). However, for the specific PPDR vertical benefit, 5G Rel-16 specifications include, and subsequent 3GPP Releases will further extend or optimize, additional features, some contributing to increase 5G own resiliency and coverage. That is the case of:

- **Sidelink (SL) communications in partial or out of coverage,** allowing terminal equipment to communicate directly [6];
- **Multi-radio dual connectivity (DC),** where terminals communicate simultaneously over different radio bearers, increasing reliability [7];
- **Integrated access and backhaul (IAB),** where 5G cell sites act both as access and backhaul for other cells, guaranteeing operation without the need for a transport network [8];
- Isolated operation for public safety (IOPS), allowing cell sites to provide a minimum set of services at their area of coverage, in case of complete isolation with the rest of the network [9];
- **5G expansion to include non-terrestrial network (NTN) accesses,** for instance, using satellite communications to extend geographical coverage to previously unreachable locations (e.g., deep valleys) [10].

In addition, 5G new radio (5G-NR) has the capacity to efficiently operate in all ranges of frequencies, with no changes in the radio interface. Thus, it may operate at higher frequencies for higher bandwidths, in an urban context, and at lower frequencies for coverage and penetration, useful in crisis scenarios. Opportunistic operation in unlicensed spectrum may also contribute to increased network availability during emergency situations. Other relevant features include user equipment (UE) power-savings features and enhancements to multimedia broadcast multicast services (MBMS) [11], based on groupcast communications. Finally, the specifications also include specific interfaces (SEAL [12] and CAPIF [13]) for applications and services to access 5G provided services, like location information. **Figure 1** shows how some of the different mentioned mechanisms fit.

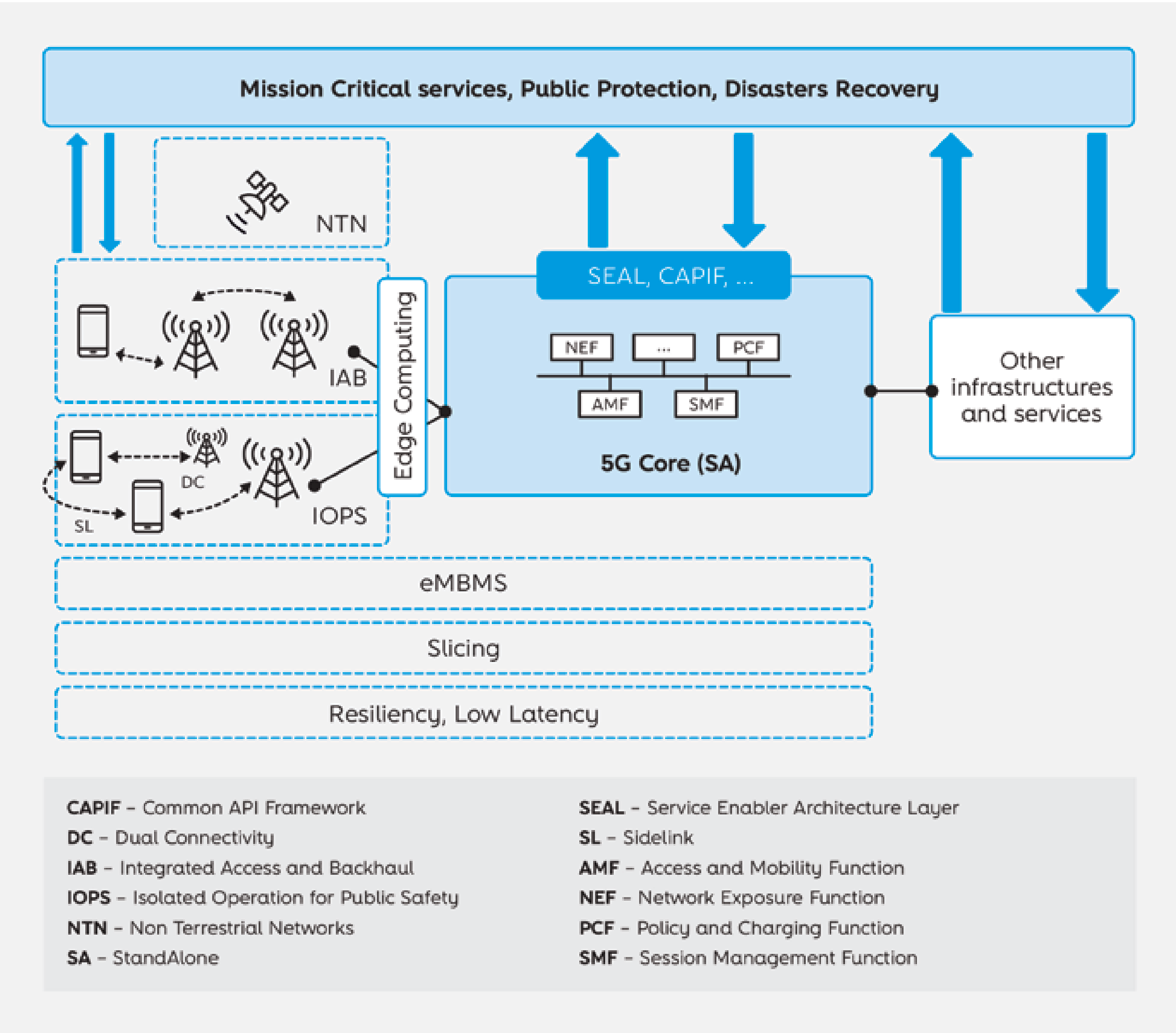


Figure 1 – Different 5G features exploitable by MCX

However, some of the mentioned mechanisms are incompatible. Specific PPDR 5G slices need to be configured with the right characteristics. For instance, accurate localization information requires 5G to operate in higher frequencies, while higher coverage and penetration, relevant aspects for PPDR in general, are obtained at lower operating frequencies. Thus, there is a need to evaluate how to compose 5G services and features for a holistic PPDR platform, serving all involved actors across the disaster cycle, from prevention to recovery.

In most countries, all the 5G spectrum is being assigned to operators. The usage of 5G by public entities for such specific public protection services requires the best service to be guaranteed, according to the requirements. Thus, one possible solution may use shared spectrum and implement a, yet to be standardized, specific PPDR vertical slice, as is already the case for vehicle-to-everything (V2X), in all operators, and a common core, independent of those. Having a mobile virtual network operator (MVNO) for PPDR is another possibility.

Another important aspect is the addition of artificial intelligence/machine learning (AI/ML) to manage 5G complexity and guarantee the best usage of 5G allocated resources. In disaster scenarios, this can help in the automated allocation of the right communication means to the involved actors.

Network edge

Under catastrophic situations, such as earthquakes, fires, or heavy storms, communications infrastructure will most likely be compromised. In such cases, it is common to have long-distance communications breakdown, with services only available locally, at the edge of the network. Albeit limited, this is still of extreme importance to local PPDR activities. The mission-critical isolated operation for public safety (MCIOPS), under specification in 3GPP for Rel.17 [9], defines the communications in such scenarios.

Besides the need to provide basic mission-critical communications, the network edge has growing importance for first responders before, during, and after emergency situations. An ever-increasing plethora of devices, like cameras, drones, and all kinds of sensors and actuators, produce huge amounts of data that need to be readily processed, analyzed, and acted upon at very short notice or even under real-time constraints, like providing haptic feedback or augmented reality. Most of these solutions rely on a mix of high bandwidth, low latency, and heavy computing that can only be found together at the network edge, in central offices and remote units, e.g., street cabinets.

Meanwhile, the networks' trend towards softwarization is transforming the network edge, once a complex ecosystem of different network appliances and connections, into something more like a data center, with standard network and computing resources [14]. As seen before, 5G communications provide a flexible and native access to these resources, featuring the need for low latency, high bandwidth, and wider connectivity options. All this is supporting the rise of the edge cloud: an extension of the cloud concepts and services to the edge of the network.

The edge cloud is today a promising work area for consumer, business, and industrial applications. Yet, its potential for domains like PPDR is evident, and many of the special needs that we can associate with public protection and disaster recovery, namely the mission-critical aspects, are currently being addressed by standards and industry fora.

In the last few years, standards organizations and industry fora have been following this reality. In particular, ETSI multi-access edge computing (MEC) defines an open architecture for "*applications from vendors, service providers, and third-parties across multi-vendor multi-access edge computing platforms*" [15], which set up a reference for the usage of these important edge resources.

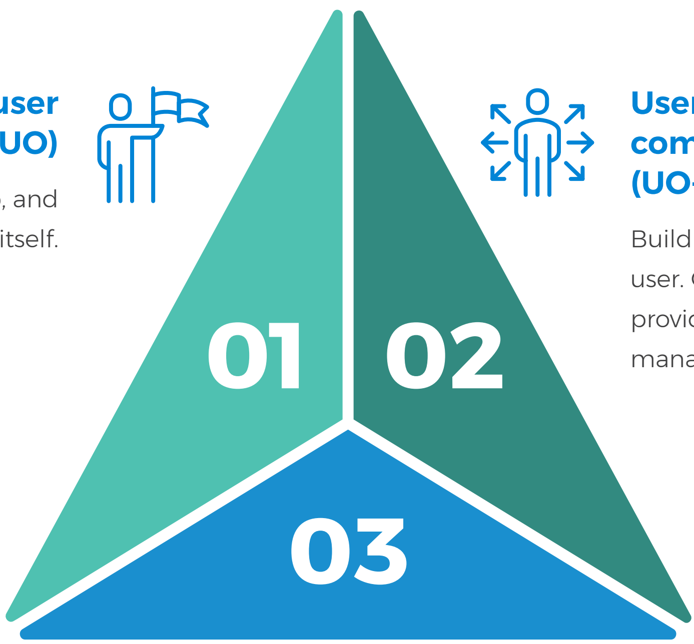
In the scope of 5G, for Rel.17, 3GPP is carrying out the studies to include standards specification for edge computing across various service/systems aspects (SA): In particular, the SA6 initiative defines an architecture that enables applications to be hosted on the edge of the 3GPP network, EDGEAPP [16], that frames the aforementioned studies. Another relevant mission-critical aspect of the edge is the IOPS [9], already mentioned.

Network operational models

A next generation mission-critical network, supported on a 5G network, requires the definition of a network operational model to be implemented at a sustainable cost. The adoption of such operational models in each country must precede an evaluation of the models that accomplish the requirements and allow for a business strategy with economic sustainability. This analysis needs to consider different perspectives like (i) spectrum management, (ii) governance model, (iii) technological model, and (iv) cost model.

The spectrum management is performed by regulators, planning spectrum assignments in dedicated or shared mode, to ensure the right balance usage amongst the various communication applications, and increasing spectrum usage efficiency, according to service requirements.

The governance model is used by national authorities to ensure that all functional requirements are accomplished with the levels of quality and safety required by this type of communications, and also to take into account economic, financial, and organizational aspects. The governance model is based on network ownership and control, and three models can be applied:



User owned - user operated (UO-UO)

Building, ownership, and operation by the user itself.

User owned - commercial operation (UO-CO)

Building and ownership by the user. Operation by a commercial provider of outsourced management network services.

Commercial owned - commercial operation (CO-CO)

User subscribes to services provided by a commercial network operator.

The technological model is used by national authorities and network operators to determine networks and spectrum sharing with public customers' services. There are three technological models applicable:

Dedicated network infrastructure: a dedicated mobile broadband network using dedicated spectrum.

Commercial network(s) infrastructure: PPDR organizations buy MCX services from a commercial mobile network operator, possibly using shared spectrum.

Hybrid solutions: based on dedicated and commercial network infrastructures, it is a shared infrastructure, which can use, or not, dedicated spectrum. In this case, there are three implementation types: i) a geographical split between dedicated and commercial network infrastructure; ii) an MVNO model where organizations share the radio access network (RAN) with the public customers, and; iii) an MVNO model with partly dedicated/partly shared RAN network.

The cost model is used by decision-makers to estimate the total cost of ownership (TCO) of a mobile cellular radio network over the long term, which includes both the initial costs to build (largely CAPEX) plus the operational costs (OPEX), and can be summarized in the following elements: the cost of the RAN, standing for approximately up to 70% of the total cost, plus the cost of the access network, representing the second-largest share of the total cost, plus the cost of OSS and BSS.

Some studies [2] [17] show a trend where next generation mission-critical networks converge to the following scenarios, relatively to the operational models that can be adopted:

Standalone

An operational model with dedicated network infrastructure, with UO-UO or UO-CO governance models and always using dedicated spectrum.

Hosted

An operational model with commercial network(s) infrastructure, with CO-CO governance model and always using shared spectrum.

Sharing

An operational model with hybrid solutions, with CO-CO governance models and using dedicated and shared spectrum.

Regardless of the scenario adopted for the operational model, three studies ([2], [17], and [18]) make it evident that if the network is not shared among several services, the TCO to provide a single service like PPDR will always be very high. The study from Analysis Mason [18] shows that the dedicated network scenario's adoption has a relative TCO much higher than that of scenarios where commercial networks are used, even with multiple backup commercial networks. **Figure 2** shows this relation. The high-ambition part also depicted includes investment in increased robustness and security compared to traditional commercial networks.

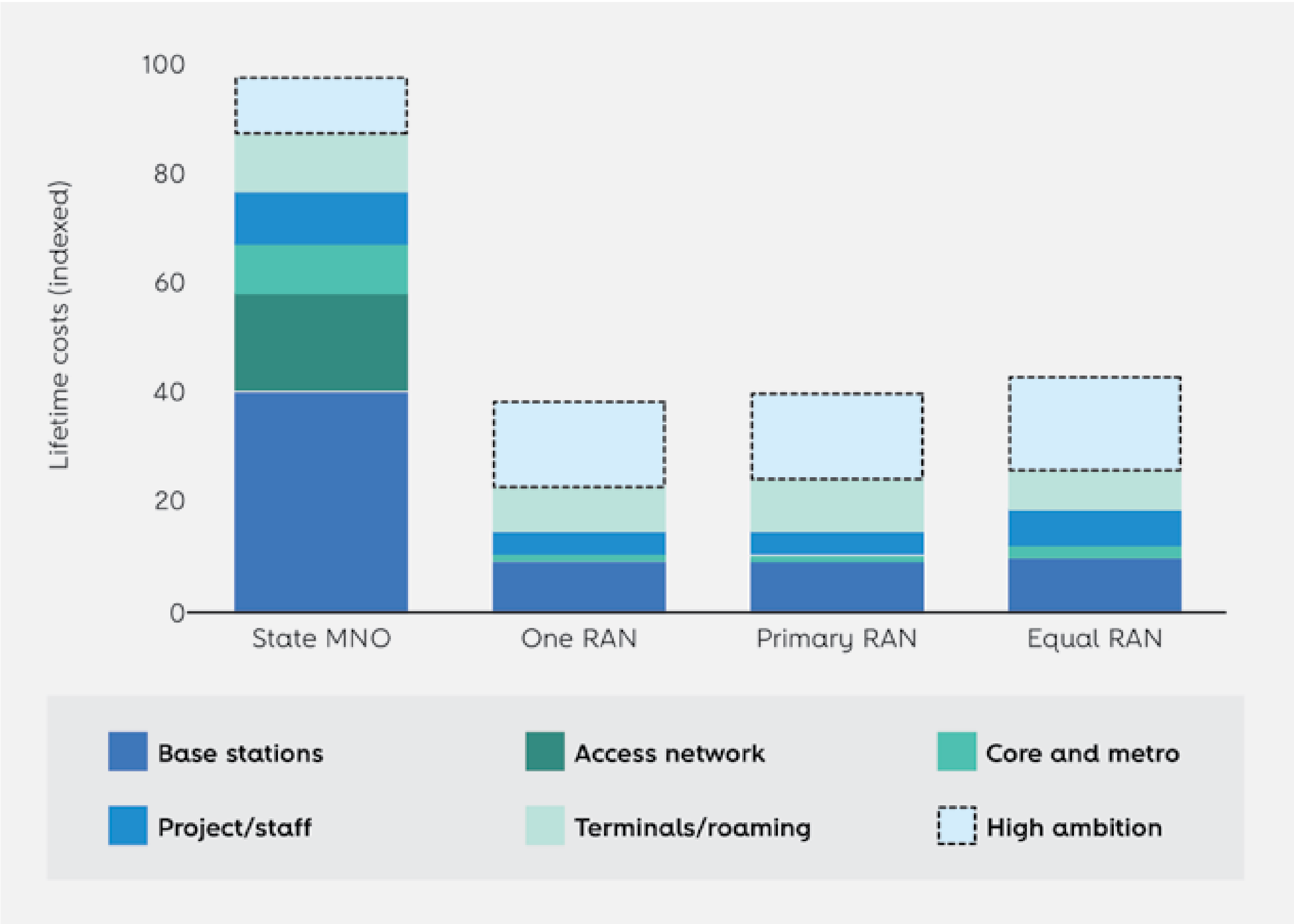


Figure 2 – Costs breakdown for next generation emergency networks using commercial mobile networks [18]

When financial funding may be an issue, the best approach would be to dilute TCO among several services, using one of the following strategies:

Specialization strategy

Use of the standalone scenario for sharing the network with other PPDR and CNI customers. CNI customers can be organizations from the utilities sector and/or intelligent transport systems (ITS) sector.

Share strategy

Use of hosted or hybrid scenarios for network sharing with public customer's services.

With the specialization strategy, it would be possible to create a specialized and dedicated network for next generation mission-critical communications services at a more affordable cost per customer.

The share strategy, more cost-effective, would allow leveraging 5G networks use cases with the same type of requirements, like autonomous cars, tactile Internet, delivery drones, etc.

However, the best operational model for next generation mission-critical communications networks will depend strongly on specific requirements and the mobile market situation in each specific country. Given the large cost differences identified above, governments and mobile network operators (MNO) need to evaluate and define a strategy to develop a robust and sustainable solution that will serve its ultimate purpose.

MNOs' role for MCX

The adoption of current commercial mobile networks to provide MCX services will lead to a lower cost per transported bit or connected user when compared with the usage of dedicated LTE networks, at a similar frequency band, for the same purpose. However, for that to be possible, MNOs need to deliver extremely high reliable, available, resilient, and secure communications, even in very adverse situations and in locations with less economic return (e.g., less population and industry).

Mobile networks supporting MCX services have to guarantee end-to-end availability above 99,999% ("five nines"), from RAN to application servers. Thus, MNOs' geographic coverage and indoor signal penetration at agreed locations must be extended as needed for mission-critical services support. Furthermore, all this network hardening and extended coverage, along with the addition of essential mission-critical functions and resilience, must be accomplished at a reasonable cost. These evolutions may also be considered business opportunities, leading MNOs to rethink their position relative to the MCX services ecosystem and other use cases that present similar requirements.

The 4G/LTE technology allows several possible alternatives to deploy a public safety LTE network, each with advantages and disadvantages, from a hosted solution to a standalone deployment, passing through various degrees of sharing with commercial networks, as mentioned before.

In the hosted solution, public safety (or MCX) agencies purchase operator services required to meet their mission-critical communications needs, minimizing the need for equipment installation and maintenance. This scenario will be supported by 5G technology, especially when 5G SA networks with slicing features become widely deployed, allowing the implementation of a specific MCX virtual network (or slice) over such commercial networks.

On the other hand, the standalone solution requires the deployment of a full network covering the service area the MCX agency is accountable for. While a dedicated deployment is attractive in terms of MCX agencies being in control of the resources and subscribers database, it comes with operational issues and higher costs to implement and maintain.

In the middle, there are various levels of models of sharing infrastructures with commercial networks: from a full connectivity solution being provided by the commercial network operator and the MCX agency connecting an application server (OTT solution) to only sharing the RAN but having a dedicated core network and service platform. The most significant advantage of these scenarios for MCX agencies is to use from the beginning the wide coverage area already provided by the RAN commercial networks, even though it needs service level agreements to ensure access to commercial network resources in case of emergency and, of course, software package upgrades are needed in the commercial network in order to guarantee mission-critical user experience.

Final remarks

This article addresses possible operators' roles regarding next generation mission-critical communications in the context of 5G and edge computing. It describes 5G main characteristics being incorporated for that purpose. This will be fully reflected in 3GPP Rel-17 specifications, expected in December 2022, making the technology well-positioned for PPDR adoption.

Edge cloud services, leveraging on 5G, pave the way to new, innovative, PPDR services and enable distributed and more resilient services platforms. Without going into much detail, network edge characteristics to support these services, in a resilient way, were presented.

5G is being tailored to be easily deployed by entities other than operators, opening the door for dedicated deployments. However, for PPDR purposes, a careful analysis, considering the presented models, shall take place in order to obtain a suitable critical national infrastructure. Different models to be taken into consideration by decision-makers were described.

In addition to the technological aspect, there are other aspects to be considered for the adoption of 5G by mission-critical communications, such as the operation of PPDR services in a collaborative way even in country border-crossing scenarios. However, until today no concrete guidelines or regulations are available for these.

Altice Portugal already has an extended geographic LTE coverage and is totally committed to continuing to implement standards-compliant network solutions. 5G will be no exception, which will enable the creation of new independent 5G logical networks, tailored to fulfill the diverse requirements of particular applications, like MCX, over the same future Altice Portugal 5G physical infrastructure.

References

[1] B. Bhatia, "Status and Trends of Public Protection and Disaster Relief (PPDR) Communications," in *ITU Regional Seminar for CIS and Europe "Development of modern radiocommunication ecosystems", 6 to 8 June 2018*. ST. PETERSBURG, 2018

[2] Directorate-General for Communications Networks, Content and Technology (European Commission), SCF Associates Ltd, "Is commercial cellular suitable for mission critical broadband?," 2014. [Online]. Available: https://op.europa.eu/en/publication-detail/-/publication/246bc6ec-6251-40cb-aab6-748ae316e56d/language-en

[3] T-Mobile Network News website, "T-Mobile Launches World's First Nationwide Standalone 5G Network", Aug/20, https://www.t-mobile.com/news/network/standalone-5g-launch

[4] 3GPP, TR 21.916, "Summary of Rel-16 Work Items"

[5] ITU-R, M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond"

[6] 3GPP, TR 23.752, "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)"

[7] 3GPP, TS 37.340, "NR; Multi-connectivity; Overall description; Stage-2"

[8] 3GPP, TS 38.401, "NG-RAN Architecture description"

[9] 3GPP, TS 23.180, "Mission critical services support in the Isolated Operation for Public Safety (IOPS) mode of operation"

[10] 3GPP, TR 38.811, "Study on New Radio (NR) to support non-terrestrial networks"

[11] 3GPP, TR 23.757, "Study on architectural enhancements for 5G multicast-broadcast services"

[12] 3GPP, TS 23.434, "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows"

[13] 3GPP, TS 23.222, "Common API Framework for 3GPP Northbound APIs"

[14] Broadband Forum, TR-384, "Cloud Central Office Reference Architectural Framework", 2018

[15] ETSI, "Multi-access Edge Computing (MEC)," ETSI, 2020. [Online]. Available: https://www.etsi.org/technologies/multi-access-edge-computing

[16] 3GPP, TS 23.558 - V0.4.0, "Architecture for enabling Edge Applications",

[17] "PPDR-TC White Paper - The Strategic Roadmap for Next Generation (Broadband) PPDR Communication Systems", PPDR-TC, 2016

[13] Harald Wium and Lie Amund Kvalbein, "Four different models for next generation emergency networks using commercial mobile technologies", Analysis Mason, 2018. [Online]. Available: https://www.analysys.com/about-us/news/newsletter/next-generation-emergency-networks-jul18/

Authors

Francisco Fontes

Senior Technology Consultant

Altice Labs, Portugal

fontes@alticelabs.com

https://www.linkedin.com/in/franciscofontes/

Rui Calé

Senior Consultant and Architect

Altice Labs, Portugal

cale@alticelabs.com

https://www.linkedin.com/in/rui-cal%C3%A9-0306132/

José António Almeida

Altice Labs, Portugal

jose-s-almeida@alticelabs.com

Carlos Pardelinha

Senior Consultant for Engineering and network operations

Altice Labs, Portugal

carlos-pardelinha@telecom.pt

http://www.linkedin.com/in/carlospardelinha

Contacts

Address
Rua Eng. José Ferreira Pinto Basto
3810 - 106 Aveiro (PORTUGAL)

Phone
+351 234 403 200

Media
contact@alticelabs.com
www.alticelabs.com