SIGMA WIRELESS

MISSION CRITICAL COMMUNICATIONS

Mission-critical communications for 2020s and beyond

Delivering future-proof next-generation public safety broadband networks

Written by global critical communications industry expert, Peter Clemons, on behalf of **Sigma Wireless.**

Version 1.1, October 2021

SIGMA WIRELESS

McKee Avenue, Finglas, Dublin 11, Ireland.

Telephone: +353 (0)1 8142100

Email: sales@sigma.ie

Web: www.sigmawireless.com

Table of Contents

1 Public safety communications in the spotlight

Public safety agencies have always had very specific communications requirements compared to commercial, mass-market consumers, due to the criticality of many of their daily tasks. Such requirements and performance metrics must obviously be delivered during the most stressful, time-sensitive, emergency situations, but also need to cater for a wide range of often mundane, repetitive tasks.

The very basic, yet ground-breaking digitalisation of most major critical communications networks during 1990s and 2000s led to the consolidation of hundreds and thousands of bespoke local and regional networks into larger, often nationwide, multi-agency networks. Across Europe, these new networks were based on ETSI TETRA (Terrestrial Trunked Radio) TDMA standards, as well as unrelated FDMA-based Tetrapol technology in a few markets such as France, Spain, Switzerland, Czech Republic – and APCO P25, mainly in North America.

TETRA, Tetrapol and P25 solutions have been specifically designed to provide highly robust and resilient mission-critical voice, status and short data communications for public safety agencies' operations, but are unable to provide many of the more modern, high-data-rate services available over commercial cellular networks. Precisely for this reason, key organisations representing the industry and community, including TCCA (The Critical Communications Association) started to engage with global standards-making body, 3GPP, back in the early 2010s, to help develop the next generation of public safety mobile broadband networks.

It has been a long journey to get to where we are today. Despite the delays and frustrations along the way, there has undoubtedly been solid progress towards a stable, mature set of standards and solutions. These are now ready to be implemented across multiple vertical industries, beyond the initial public safety remit, promising significant economies of scale, a future-proof roadmap of continuous development and enormous potential societal benefits.

Here in late 2021, following a prolonged global health crisis and the steady emergence of a new world enabled by digital transformation and advanced technology, public safety agencies can confidently deploy critical communications solutions based on global standards. 3GPP-based 4G/LTE networks continue to be enhanced and will eventually be replaced via relatively straightforward software upgrades by the latest 5G configurations and architectures, future-proofing existing investments.

Organisations setting out on this journey or in the early stages of putting together requirements now have access to a large amount of information about global best practices. Technology, business models and operational practices continue to evolve. We are at the beginning of a long journey towards ever-refined, ever-improved solutions that will save time, money and lives.

This White Paper is a brief introduction to some of the major issues, trends and considerations that public safety organisations need to take into account to avoid certain pitfalls, embrace meaningful change and steer their stakeholders and end-users towards a better, smarter, safer future.

I would like to thank Sigma Wireless for the opportunity to publish this document which I hope will help the wider community make the best possible informed choices moving forward. We are also here to answer any questions you may have and help you with future deployments.

Source: Sigma Wireless Communications 2021

2 Comparing TETRA, standard MNO & mission-critical LTE for public safety services

Before presenting some of the major trends on the road to full 5G public safety networks in Chapter 3, and then explaining a number of key issues to be considered while making this generational switch to 3GPP-based technology in Chapter 4, we will begin this White Paper by comparing the main existing and future options: to see how far we still have to go, whether or not standard mobile network operators (MNOs) can provide such functionality (spoiler alert: we don't believe they can!) and whether or not the right mission-critical LTE solutions can.

The road from standard public safety narrowband networks (i.e. TETRA) to broadband ones (i.e. LTE and future 5G) is proving to be a long, arduous, often painful one for pioneer countries and agencies. ETSI-standard TETRA technology has been so successful in its adoption and operation for close to 2 decades now across European and international markets that public safety agencies and their users are extremely reluctant to migrate to (and more importantly, depend upon) next-generation solutions until these can provide the full range of services at the required service level that they have come to expect from TETRA.

As we can clearly see in the following table, standard mobile operator networks have not been designed to cater for public safety's mission-critical needs. Fortunately, extensive standards work within 3GPP and product development on a global scale from multiple leading equipment manufacturers and solutions providers have created mission-critical LTE solutions that are maturing rapidly and now being deployed at scale across Europe and globally. By the mid- to late-2020s, it is expected that a significant proportion of public safety agencies will have either migrated or be in the process of migrating all their critical communications services to 3GPP-based solutions.

It is important to highlight that this full migration will also depend upon the availability of sufficient sub-1GHz spectrum – and preferably frequencies as close as possible to existing TETRA spectrum in 380-400 MHz, such as 410-430 and 450-470 MHz for full re-use of existing TETRA sites for full broadband coverage. Allocations in 700 MHz – and 600 MHz before the end of this decade – would also be highly beneficial to the public safety community.

Key criteria comparison between TETRA, standard MNO & mission-critical LTE networks			
	TETRA	Standard MNO	Mission-critical LTE
Landmass focus	X		X
Population focus		X	
One-to-one comms	X	X	X
One-to-many comms	X		X
Broadband data		X	X
Video-streaming		X	X
Mission-critical PTT	X		X
Mission-critical data/video			X
Basic M2M	X	X	X
Industrial IoT			X
E2E Cybersecure	X		X
Significant overlap coverage	X		X
Deep, in-building coverage	X		X
In-building relying on WiFi		X	
<350ms call set-up time	X		X
Multi-agency talk groups	X		X
Ground-to-air comms	X		X
20km. out to sea	X		X
Resilient switching/backhaul	X		X
Direct mode	X		Future roadmap
Independent power source	X		X

Source: Sigma Wireless, Quixoticity-EU (Based on standard requirements/deployments)

3 Major trends on the road to full 5G public safety networks

In this chapter, we begin by profiling the major global mobile broadband standards-making body, 3GPP, which brings together all the major telecommunications companies and institutions, often competing fiercely against each other in the global market-place, but working together towards the common goal of global standards. 3GPP has been defining global mobile communications since beginning work on 3G back in 1998 – and mission-critical communications standards since tackling group call and device-to-device enablers in Release 12 from around 2012.

We then look at the progress and current status of pioneer critical broadband projects in North America, Europe, Middle East and Asia-Pacific, who are all developing and delivering major communications networks based on these 3GPP standards, as well as presenting expected timelines for full implementations, as set out by global associations such as TCCA.

The remaining sections are then dedicated to 3 hot communications technology trends (among many): OpenRAN, 5G Core and private networks. Such technologies and the initiatives developing them, are all defining the rapidly emerging 5G Era, which should lead to greater openness, competition, transparency, and innovation within the wireless space. Such efforts should also allow them to play an increasingly important role in accelerating and enhancing the next generation of public safety and mission-critical communications solutions.

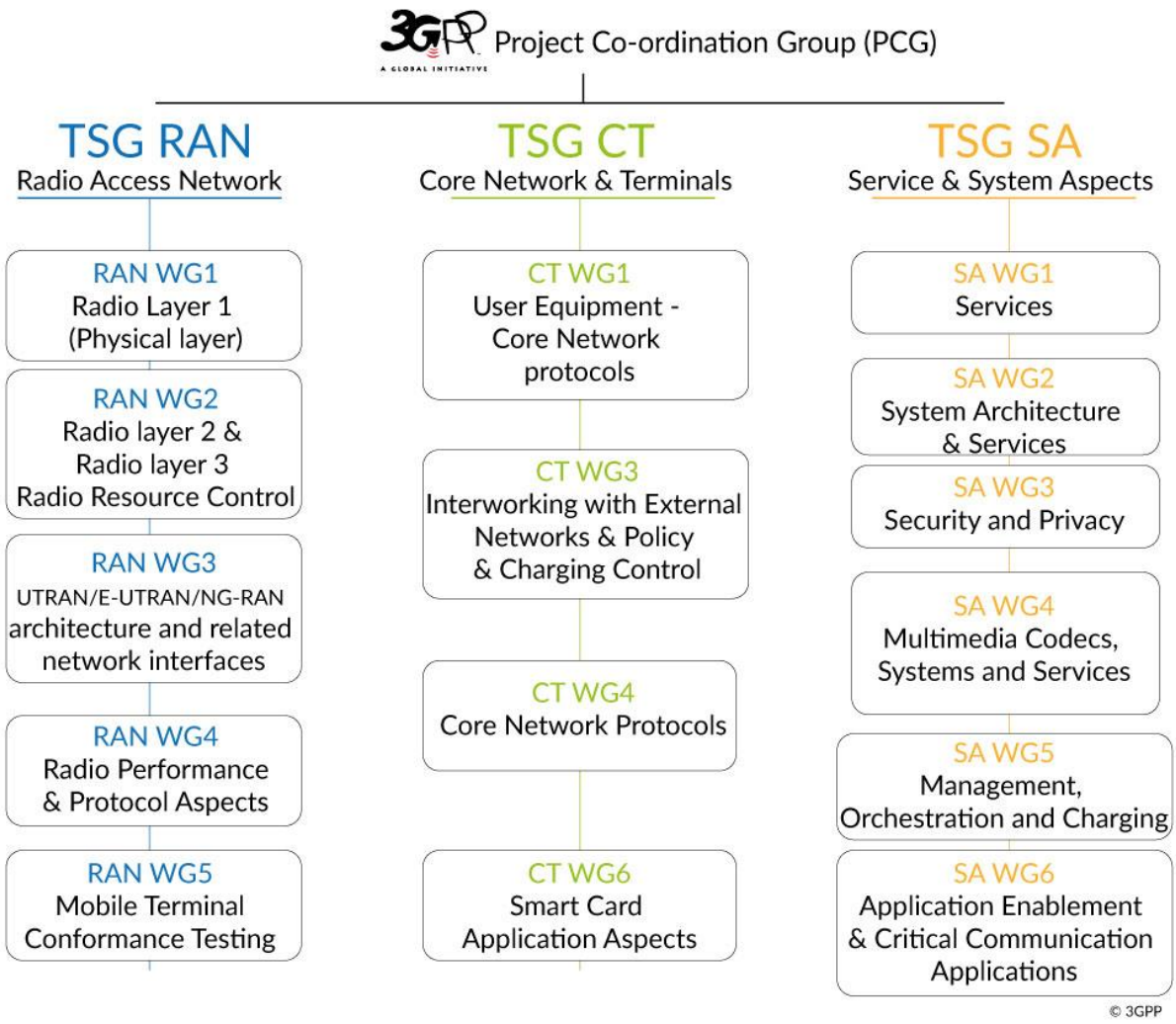
3.1 Importance of 3GPP

3GPP (Third Generation Partnership Project) was set up in 1998 by the main regional telecommunications standards bodies from Europe, Americas and Asia - (ARIB, ATIS, CCSA, ETSI, TTA, TTC) with Indian body, TSDSI, joining in 2014 – to develop the first truly global mobile broadband technology, UMTS/3G. LTE/4G followed from Release 8 in 2008, with 5G standards officially sanctioned from Stage 1 Release 15 onwards in Q4-2017.

3GPP is divided into 3 main Technical Specification Groups (TSGs): RAN – Radio Access Networks, SA – Service & System Aspects and CT – Core Network & Terminals, with each TSG containing multiple Working Groups (WGs) as outlined below, following a complex waterfall model where RAN deals with all Stages, and in particular Stages 1 & 2; SA1 deals with Stage 1 and SA2/SA6 looks at Stage 2, SA3 is entrusted with all security issues; SA4 codecs and multimedia; SA5 management, billing etc., while CT then completes each technology Release at Stage 3.

RAN1 deals with the radio access physical layer, while RAN2 deals with higher software layers, RAN3 with architecture and interface issues, with RAN4 looking at overall performance, including spectrum and RAN5 conformance testing.

The global public safety industry became active within 3GPP around 2012 with Release 12 (LTE Advanced Pro), where some key functionality was added to enable better group calling and direct mode (Proximity Services/ProSe via PC5 interface). The importance of the public safety industry in 3GPP's future roadmap was recognised in late 2014 with the creation of the first new Working Group – SA WG6 (SA6) - to be added since 3GPP's inception in 1998. SA6 is now the focal point for Stage 2 work for all vertical industries (following the reception of requirements study items within SA1) and application-level work items within 3GPP.



As can be seen in the graphic below, Release 13 was the true starting-point for mission-critical services, with the development in just over a year, from January 2015 to March 2016, of a full suite of mission-critical push-to-talk (MCPTT) standards, building upon the OMA PoC standards work carried out previously and adapting these to public safety requirements within the 3GPP framework.

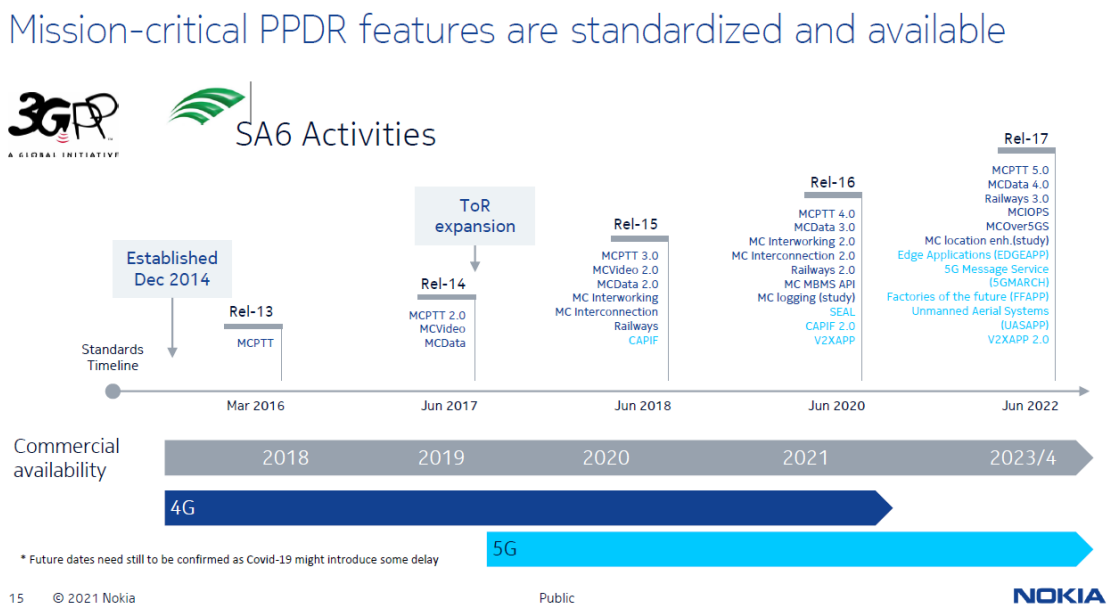
Release 14 saw the consolidation of essential mission-critical features in a separate document and the addition of mission-critical data and mission-critical video standards. Due

to the ongoing nature of 3GPP Releases, this basic suite of mission-critical services (MCX) continues to be added to and enhanced in future releases all the way to the current Release which we are working on during mid-2021: Release 17.

Release 15 also saw the development (Stages 1 & 2) of work on an interworking function (IWF) from both 3GPP (LTE-side) and ETSI (TETRA-side) – also ATIS work on P25-LTE interoperability based on P25 ISSI interface - to allow essential interoperability between legacy TETRA/LMR systems and mission-critical LTE systems. Guaranteed interoperability between multiple mission-critical systems was also standardised, as well as common API functions and multicast-broadcast APIs.

Release 16 completed Stage 3 work on IWF as well as continuing work for new verticals such as railways, industry 4.0, drones, automotive etc. This release also included important extensions to the overall applications environment including Edge/MEC, private networks, satellite systems as well as guaranteeing the smooth migration of all mission-critical services to 5G and beyond. Release 17 adds more functionality and so on.

During second half 2021, 3GPP will discuss requirements for Release 18, the first release of 5G Advanced, where even more services benefiting the public safety and other critical industry sectors are expected to take centre stage as global societies and economies continue their digital transformation as we emerge from the current global health crisis.



Source: NOKIA, 3GPP

3.2 Pioneer public safety networks and expected timeline

As mentioned earlier, most European Governments and public safety agencies have been relying on nationwide TETRA and Tetrapol networks for their basic mission-critical communications needs. High-speed data, video and other advanced services are not available over such platforms and no further development is taking place to keep them up to date with latest and future user requirements. Following the industry's engagement with 3GPP to develop next-generation solutions, several pioneer countries' agencies from around the world have developed and are implementing major programmes to enhance, update and ultimately replace their legacy systems.

United States of America - FirstNet

Following lengthy enquiries and extensive lobbying by the public safety community during the aftermath to 9/11 attacks in 2001, the First Responder Network Authority (FirstNet) was set up in 2012 aided by the award of 2x10 MHz 700 MHz (Band 14) spectrum and access to up to US$ 7 billion to drive forward a nationwide public safety broadband network across USA.

Following further lengthy consultation and tender processes, AT&T was awarded a 25-year contract in 2017 to build and run the network on behalf of public safety. Existing state-wide P25 networks will continue to operate for mission-critical voice service, i.e. LMR PTT, but FirstNet has already been successful in attracting over 2 million users for mission-critical broadband service, as well as adopting standards-based MCPTT and announcing future migration to a 5G core. AT&T is also offering first responders priority access across all commercial spectrum and network assets.

United Kingdom - ESN

UK Home Office's Emergency Services Network (ESN) is being built as part of ESMCP (Emergency Services Mobile Communications Programme). The original contracts, awarded in late 2015, were divided into 4 lots, with KBR, a consulting company awarded Lot 1, Motorola Solutions awarded Lot 2 to develop separate core network and mission-critical services and EE, now part of BT, awarded lot 3 for mobile network services. Arqiva won Lot 4 for extended coverage, but UK Home Office decided that it would work directly with Lot 3 winner to build extra sites in remote locations.

Originally planned to replace the existing Airwave TETRA network (also now owned by Motorola Solutions) in 2016, the TETRA switch-over was originally delayed until end-2019, with further extensions until 2022, 2025 and now end-2026. UK ESN has been watched very closely by other public safety agencies around the world to learn the lessons from such a challenging "big-bang" process, which was abandoned in early 2020 for a more incremental, staged approach.

Korea - SafeNet

Following a well-publicised ferry disaster in April 2014 where hundreds of citizens, including schoolchildren lost their lives, the Korean Government decided to invest significant resources in building a new public safety communications capability, based on the emerging 3GPP standards. SafeNet is actually 3 separate networks rolled into one: a terrestrial public safety LTE network, an LTE network for railways and a maritime network. Dedicated spectrum has been awarded in 700 MHz Band 28 and the service is now being rolled out across the Republic of Korea.

Finland – VIRVE 2.0

In Finland, Government-owned operator, Suomen Erillisverkot runs the nationwide TETRA network, VIRVE. A next-generation public safety mobile network project was set up in 2017, but no dedicated spectrum was made available for the new service, so Erillisverkot will need to work with mobile operators to deliver its mobile broadband service. In 2019, the law was changed to allow national roaming in Finland so that public safety has access to multiple networks. In March 2020, a contract was awarded to Ericsson to build a dedicated public safety core and another contract was awarded to mobile operator, Elisa, to provide nationwide RAN services to Erillisverkot. It is expected that data services will be available during 2022 and full migration from TETRA to LTE/5G should be complete by 2025.

Middle Eastern region

The Middle East region is at the forefront of developments in public safety broadband:

Qatar Ministry of Interior was the first agency in the world to deploy a public safety LTE network on dedicated 800 MHz Band 20 spectrum in 2012.

Nedaa is deploying a public safety network with dedicated spectrum in 700 MHz and 2.3 GHz across Dubai to enhance and eventually replace the existing TETRA network.

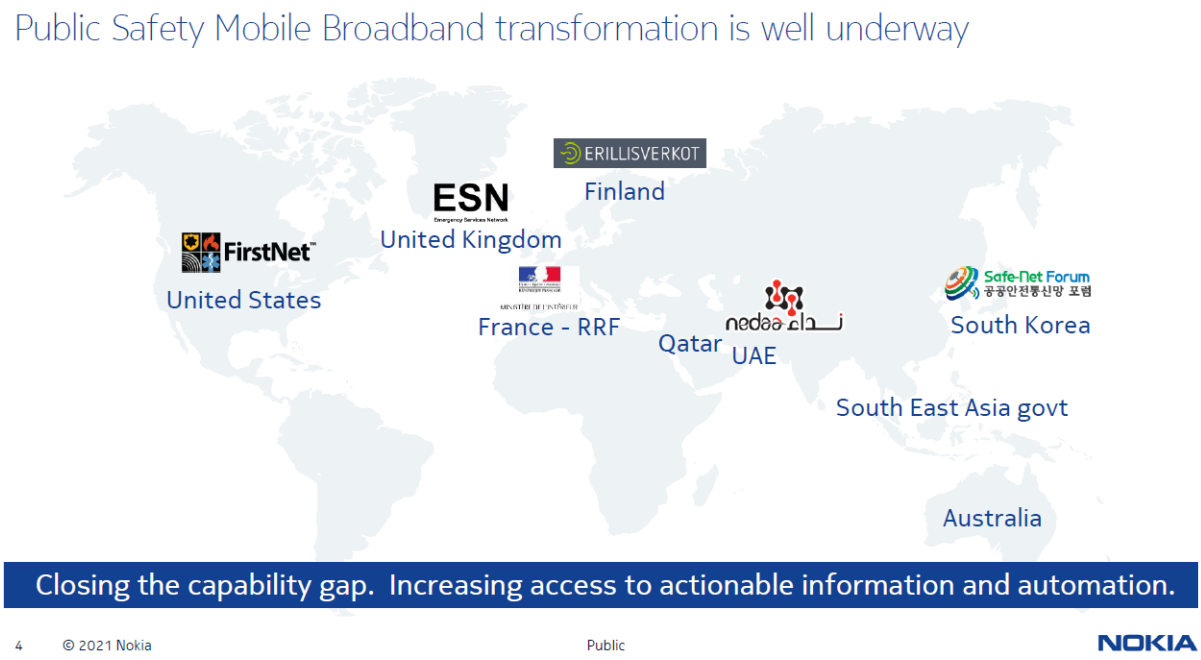
France – RRF/ACMOSS

French Ministry of Interior launched a tender for a nationwide public safety network to replace its existing Tetrapol networks during late 2020 and is currently in the process of awarding contracts for 3 Lots: RAN to at least 2 mobile operators; core and associated services to a systems integrator; and a smaller contract for IT/network management.

It is hoped that the nationwide public safety network will be up and running in time for 2024 Paris Olympics, with early coverage in major cities for 2023 Rugby World Cup and all 300,000 public safety officials and related users on the network by 2025. During 2021, it was announced that a new agency – Security and Public Safety Operational Mobile Communications Agency - (French acronym -ACMOSS) is being set up to run operations when the network goes live.

Australia - PSBN

In Australia, New South Wales (NSW) Telco Authority is leading the procurement of a nationwide public safety network capability (PSBN) on behalf of all states. Following a lengthy consultation and procurement process beginning in 2017, in April 2021 it was announced that a pilot/trial network is being set up and built by Nokia that will use both TPG and Optus mobile networks to test the feasibility, functionality and redundancy of a future public safety network.



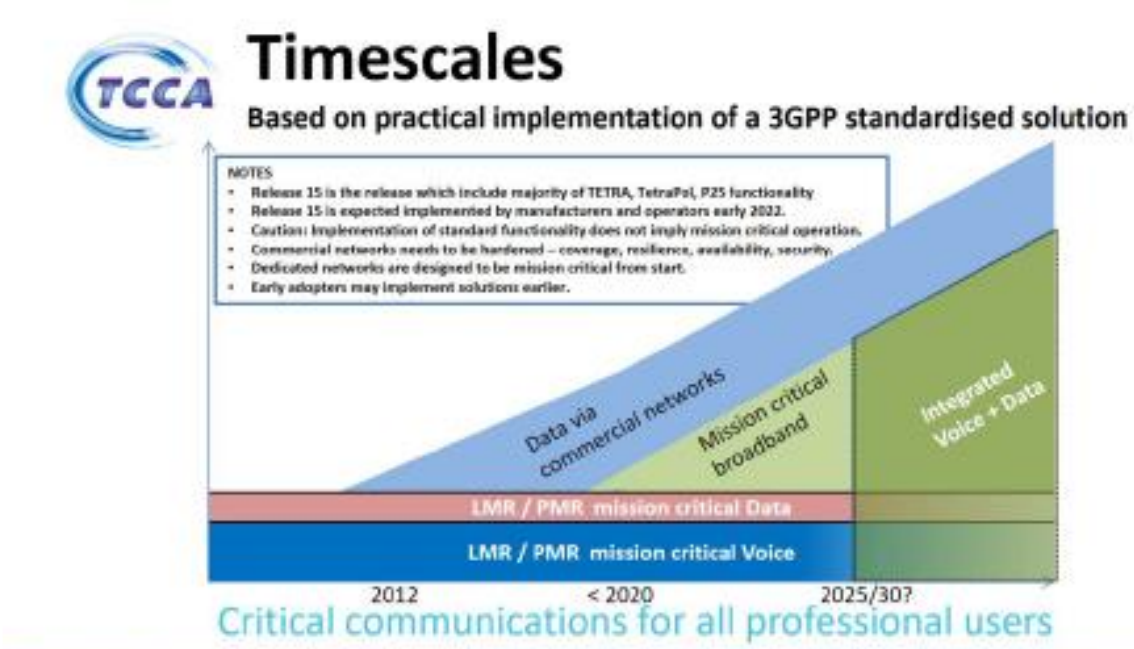
Source: Nokia

As we have seen, looking at the experiences so far of certain pioneer nations, it can take up to 10 years – or even longer - to deliver a fully-functioning next-generation critical communications platform. It is therefore important to start preparations early, engage with end-users and the wider global community, to increase the chances of ultimate success.

As we move towards more agile, flexible, CI/CD frameworks (see trends below in sections 3.3, 3.4), public safety organisations need to change their structures and procedures to fit into the new digital transformation dynamic of modern systems. Public safety organisations are conservative by nature, often with good reason, where public health and safety is on the line, but they also do not operate in a vacuum and must keep up with major trends in wider society, to attract the next generation of first responders.

Having developed an initial timeline for migration from TETRA to LTE back in 2012, when its Critical Communications Broadband Group (CCBG) was first set up, TCCA recently (2018/19) updated its timeline to account for more recent developments, setting 3GPP Release 15 (5G Phase 1) as the baseline for full, basic mission-critical services over hardened 3GPP networks.

Existing TETRA networks are likely to continue until at least 2025, with most existing systems reaching end of life/support by 2030. Public safety organisations have already been using commercial networks for non-mission-critical data since as early as 2012, with the switch to mission-critical broadband data now currently under way in pioneer markets. By 2025, we should see several nationwide public safety broadband networks integrating full mission-critical services (voice, data, video and multimedia) with the vast majority of the community adopting complete solutions over the following 5 years.



Source: TCCA

3.3 Open RAN

Large-scale commercial – and their critical equivalent - networks have become progressively more complex, expensive and tightly integrated as we have moved from 2G to 3G, 4G and now 5G. This has led to supplier consolidation within the global mobile communications industry with a very small number of companies capable of delivering such large-scale, predominantly best-effort networks to mobile operators.

Geopolitical tensions have also led many Western Governments to legislate against high-risk vendors (HRV) – particularly Chinese vendors in Western countries - being used for the next generation of radio access and core networks. Initiatives have been under way for the past

few years to open up the closed interfaces within modern communications networks, enabling and encouraging new players to enter the market, driving innovation and cost reductions as operator margins wither.

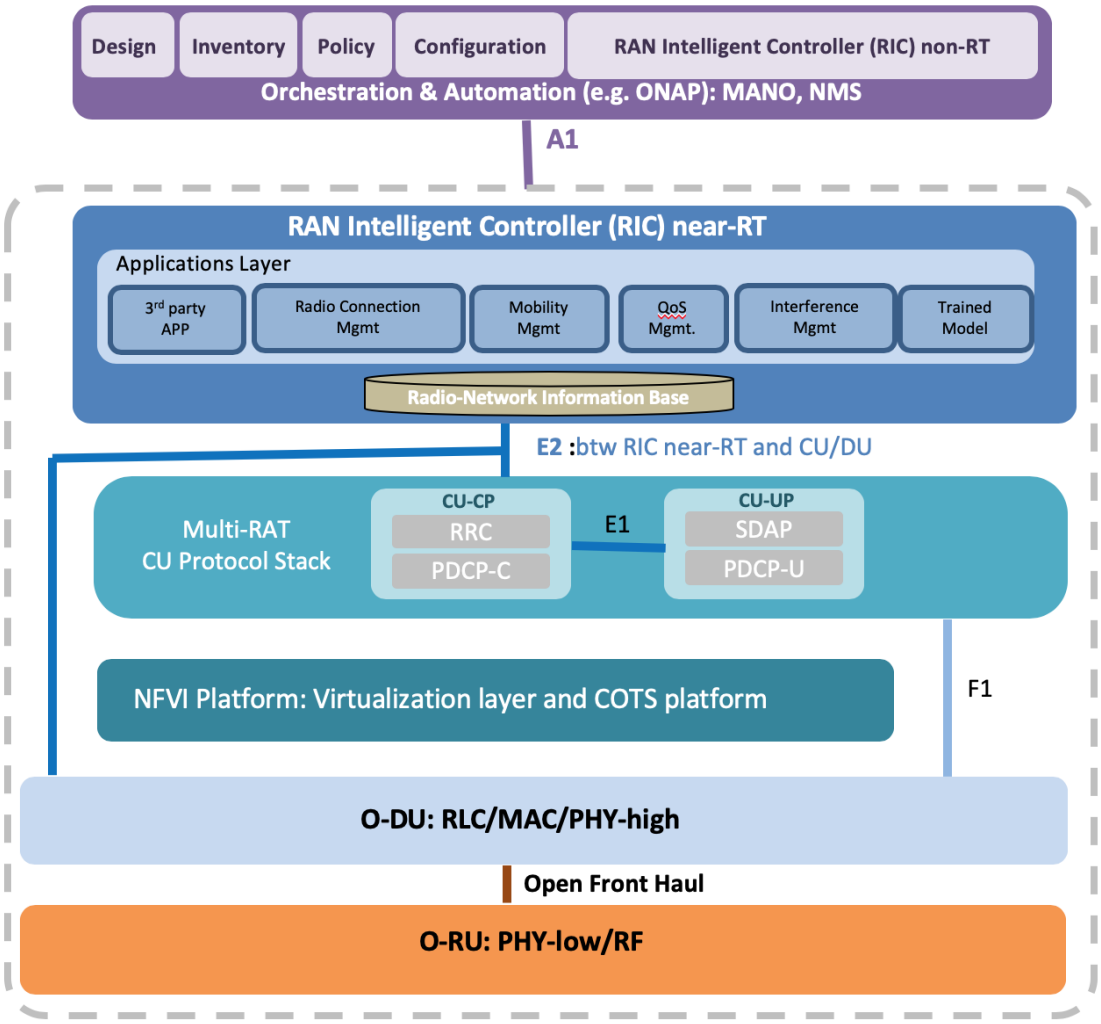
Some progress towards greater openness and network disaggregation has already been made during the implementation of LTE Advanced networks during mid- to late 2010s. Higher-layer RAN functions are being centralised in operator data centres in cloud RAN and virtualised RAN configurations, allowing mobile operators to reduce costs, simplify tower-site deployments and encourage supplier diversification. Signalling and media flows have also been decoupled to a certain extent, allowing more efficient use of resources and flexibility in the placement of network functions.

5G presents the perfect opportunity to accelerate these trends, allowing public safety agencies, industries and specialised service providers to have access to a much wider range of services, including fully isolated network slices, delivering more secure, responsive, dedicated resources. Ultimately, the disaggregation and simplification of 5G network design allows public safety and public service agencies to retain greater control over their networks, in a similar fashion to legacy narrowband PMR networks, especially if private spectrum resources are also made available by the relevant authorities.

New industry organisations such as Telecom Infra Project (TIP), O-RAN Alliance and even open-source communities such as those at Linux Foundation, Open Networking Forum (ONF), Cloud Native Computing Foundation (CNCF) etc., are working on a growing number of projects and initiatives that will benefit critical communications end-user communities. The networking landscape is being radically transformed, with significant investment in powerful, cloud-native, fully virtualised and automated solutions based on the very latest network architectures and principles. Industry standards bodies then incorporate these advanced architectures into the latest 5G releases, ultimately benefiting the public safety community and other verticals.

As can be seen from the classic O-RAN Alliance OpenRAN architecture pictured below, multiple open interfaces are being developed by smart people working for networking industry giants, start-ups and academic institutions alike driving more powerful, flexible software-defined approaches. This leads to greater convergence, intelligence, automation, control, customisation and visibility that opens up the previous radio access black-box to greater scrutiny and greater potential for future solutions.

Within the OpenRAN framework, RAN is split into 3 separate units: RU (radio unit), DU (distributed unit), CU (central unit), and AI/ML control/automation made possible with the introduction of near-real-time and non-real-time intelligent controllers (RIC). This is all wrapped into an orchestration and automation framework (SMO) containing multiple feedback loops, allowing enterprises, public safety agencies and specialised critical communications service providers much greater control, accountability and visibility into the network.



Source: O-RAN Alliance

Clearly, it is still very early days for this Open RAN movement and many challenges remain to be solved. A greater number of interfaces, potential suppliers and a longer, more diverse and geographically dispersed supply chain creates new security threats, integration challenges and new opportunities for lock-in at the system integrator or even chip-set/essential component level. However, open RAN will also undoubtedly encourage faster innovation, new services, greater intelligence and more control and visibility over previous black boxes, allowing public safety agencies to explore new, more flexible business and operational models that reduce costs, complexity and deliver better outcomes.

3.4 5G Core

The brain of the network, the mobile core, is also undergoing significant changes within the 3GPP framework as the industry looks to deliver a much wider range of services while moving from 4G-LTE solutions towards a full 5G network architecture. This important

development is likely to lead to significant changes to the way networks are built and operated within the timeframe of public safety agencies' migration from TETRA to full 3GPP.

Circuit-switched GSM/2G solutions were originally optimised for voice communications, with packet data incorporated with GPRS. UMTS/3G solutions started to offer differentiated voice and wideband data, whereas LTE/4G switched to an all-IP enhanced packet core (EPC). More and more functions were added to the control plane/signalling part of the network. In an attempt to manage the growing complexity, concepts such as NFV – network functions virtualisation – and SDN – software-defined network – were introduced to move away from a hardware-based, separate boxes approach to a more manageable – in theory – end-to-end, software-based approach.

Once again, just as in the case of the radio access network, 5G is seen as an opportunity to re-think how mobile networks are built, with many of the advances able to be retrofitted to existing LTE networks, especially those based on more recent 3GPP releases.

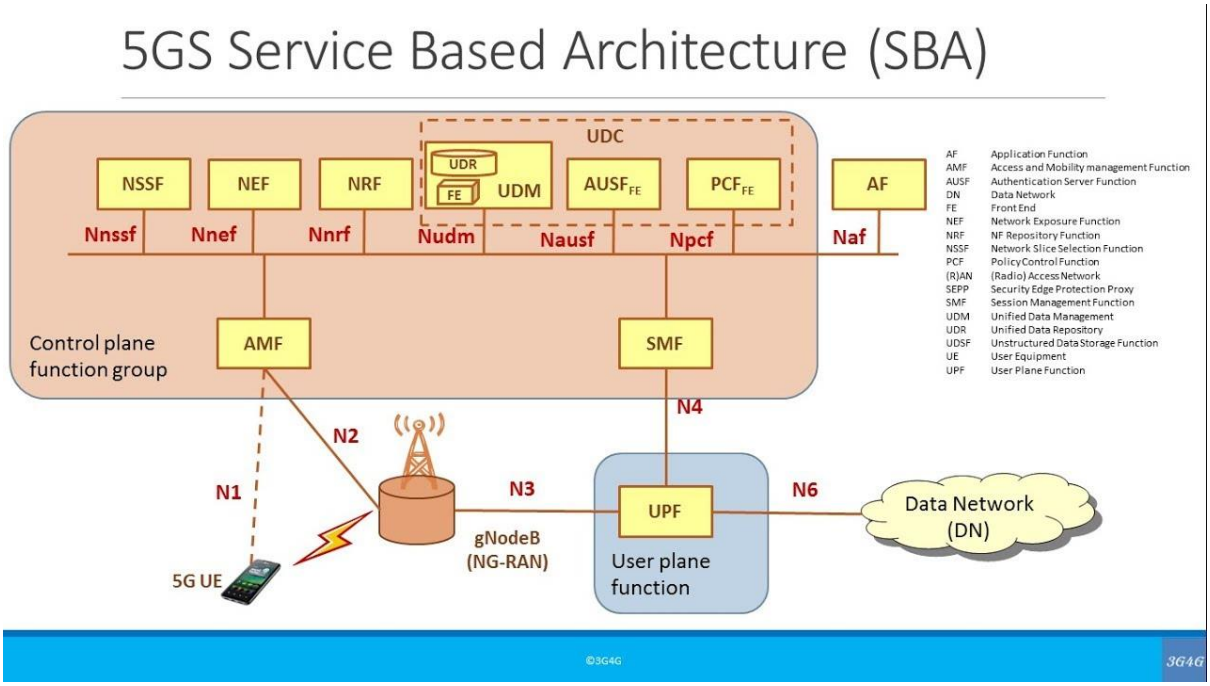
5G continues the trend towards control and user plane separation started during LTE. This allows many of the non-real-time control and signalling functions to be centralised in a data centre where a more IT/cloud-like service-based approach allows the different network functions to communicate with each other over a common services bus using standard HTTPS protocol, rather than the increasingly limited and unmanageable one-to-one reference points based on specialised protocols used in the past. The user plane is consolidated into single or multiple UPFs (User Plane Functions) that can be placed at the most appropriate point across the network to allow higher-throughput, lower-latency, more-efficient data transmission than was previously possible.

The new 5G SA Core also enables end-to-end network slicing, where one physical 5G infrastructure can be managed, orchestrated and automated for multiple, fully isolated logical networks for different users, use-cases and purposes. As well as serving mobile network operators looking to increase their range of services and profit margins, network slicing also allows private network operators to separate out mission-critical traffic from non-mission-critical, as well as keeping all sensitive data within the boundaries of their own network.

As next-generation radio access and core networks start to behave more like the Internet and clouds of the IT/hyperscaler worlds, more options and new services become available to enterprises, Governments and public safety organisations. It is important to stay informed of the latest developments in this rapidly changing environment and avoid being tied into expensive, static, long-term, proprietary solutions.

Once again, as in the case of open RAN, the full development of stand-alone, disaggregated 5G core solutions is still in its early stages and many challenges must be overcome to allow such solutions to control next-generation public safety networks. Traditional vendors and mobile operators still control much of the global standards and R&D efforts, making backward compatibility a challenge.

However, many analysts believe that 5G stand-alone cores could actually be deployed first in private networks for mission-critical industrial processes, with little legacy cellular equipment to worry about. This is an area where standards and solutions are developing fast, so the public safety community must make sure it keeps up to date with developments and contributes to the debate where possible.



Source: 3G4G

3.5 Private networks

Governments and public safety agencies across the world have been used to commissioning, deploying and maintaining their own private networks for decades. However, as the costs and complexity of deploying the most advanced technology solutions has risen sharply in recent times, more and more agencies have been looking to outsource key capabilities to network operators and systems integrators.

Since the advent of 5G in 2018 and as each new Release progresses, new, more flexible, hybrid models are becoming available. Within 3GPP standardisation, several items regarding NPN (non-public networks) have been and continue to be worked on by a growing number of verticals, with a particular interest from Industry 4.0 players from associations such as 5G-ACIA and 5G IA, who need very high reliability and low latency to operate complex, mission-critical processes within factories and campuses. More service providers and system integrators are specialising in the deployment of private networks, that can either be stand-alone or integrated with public networks RAN, core, transport networks or combinations thereof (see graphic of different options below).

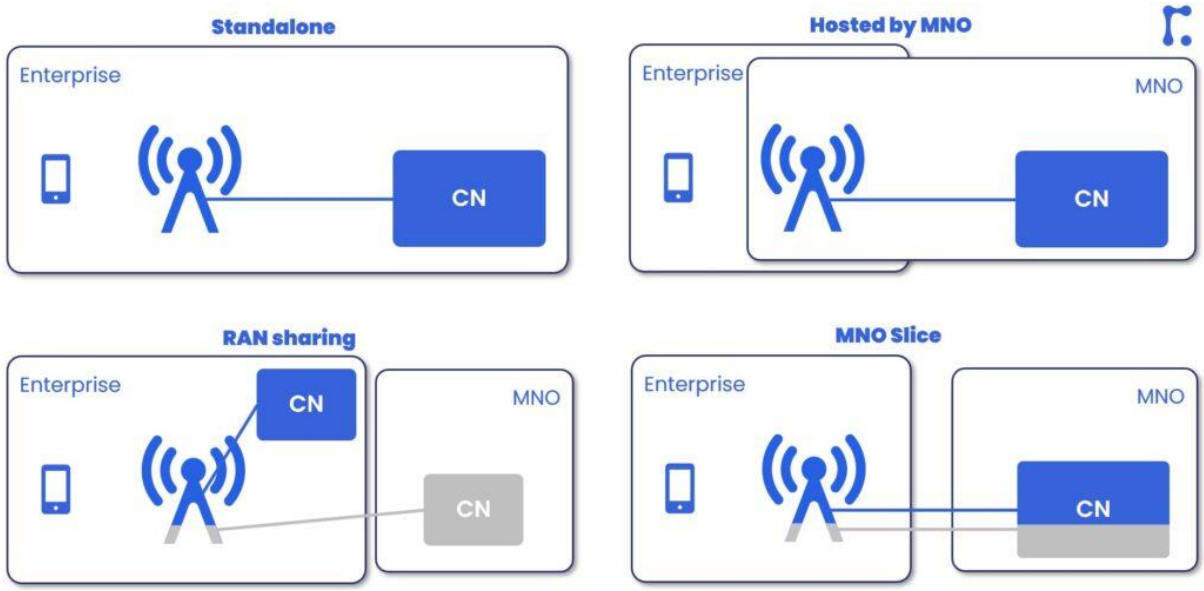
Previously, all 3GPP spectrum - in a limited number of popular frequency bands standardised on a regional and global level - has been awarded or auctioned off to highest-bidder mobile network operators, giving them exclusive access to build best-effort nationwide networks. Recently, many countries in Europe, North America and Asia have been assigning allocations of 3GPP-compliant spectrum for local or regional private networks - 40 MHz of 2.6 GHz TDD Band 38 in France; 100 MHz of 3.7-3.8 GHz C-Band spectrum in Germany; multiple bands in UK; 3550-3700 MHz (CBRS) in United States - allowing healthy private network ecosystems to emerge.

In multiple European nations, parts of 700 MHz (Bands 28A/68) have also being awarded to public safety on either side of Band 28 spectrum being auctioned to network operators, with chip-sets, devices etc. slowly becoming available to facilitate future deployments from mid-2020s. Ecosystems of utilities and other critical users are emerging in the traditional PMR 400 MHz bands (450-470 MHz – Bands 31, 72 & 410-430 MHz – Bands 87/88) to allow wideband/broadband applications – 2x3 or 2x5 MHz - such as massive IoT.

Many industry experts believe that the most cost-effective manner of building next-generation public safety networks is for Governments and agencies to partner with mobile network operators providing priority and pre-emption and guaranteed service levels over existing spectrum assets. However, new private network solutions are being actively promoted by public safety and industrial players as part of global 5G standards, making dedicated or hybrid mission-critical-grade networks increasingly feasible and affordable in the future.

Dedicated spectrum in sub 1-GHz for wide-area coverage and guaranteed service paired with dedicated spectrum in mid-band (European Commission is studying 3.8-4.2 GHz for future private 5G services) for additional capacity for future services, could also be combined with public network spectrum for offloading non-mission-critical traffic within 3GPP NPN framework. Therefore, increased availability of dedicated spectrum for public safety users is likely to be a key factor in the delivery of secure, robust, resilient mission-critical services within the 2025-30 timeframe.

Returning to the graphic below showing NPN options mainly for enterprise, industrial and campus deployments within 3GPP documentation, only the initial, top-left standalone option provides public safety and other mission-critical users with guaranteed SLAs/KPIs allowing them to complete their mission. However, for reasons such as cost and spectrum availability in certain markets, MNO networks and related assets might be required from Government and public safety agencies. If this is the case, comprehensive risk and security assessments will need to be conducted.


Standalone
Enterprise
CN
Hosted by MNO
Enterprise
MNO
CN
RAN sharing
Enterprise
CN
MNO
CN
MNO Slice
Enterprise
MNO
CN

4 Public Safety Network Checklist

Each procurement of a next-generation public safety broadband network will be unique to the specific background, history, circumstances and future requirements of individual markets, institutions and agencies. However, after a decade or so developing and maturing requirements, standards and deployments globally, clear trends and best practices are emerging as each new programme is designed and deployed.

After a couple of decades of incremental change in public safety communications networks, following the introduction of the early standards-based nationwide TETRA solutions across much of Europe and elsewhere during early 2000s, we are now entering a new era of upheaval – aka rapid innovation and new opportunities - for first responders. This requires new, more powerful and future-proof systems to be deployed that can cope with the challenges of the next two decades. In this rapidly changing environment, there is an even greater need to have a solid, yet flexible plan in place allowing necessary adjustments to be made during the programme's execution.

This chapter starts by looking at some of the key legal aspects to be considered during the migration from narrowband to broadband networks. Understanding the current and future capabilities of the chosen technology is critical, as well as making sure sufficient spectrum is made available to accommodate existing and future services. We then look at the network architecture and the wider range of services themselves that will be deployed over next-generation networks.

Further sections are dedicated to how full coverage can be achieved as well as full service availability, as we are dealing with mission-critical, public safety networks that must never fail, especially during the most extreme situations which unfortunately seem to be hitting modern societies with increased frequency. Following a section dedicated to all-important security aspects, we end with a look at how cost-conscious Governments and public safety agencies can fund these new systems and keep equipment and running costs as low as possible while delivering high-quality public services.

Public safety communications in the 2020s and beyond is such a complex, multifaceted "programme of programmes" that we can only start to scratch the surface of all the topics to be discussed and resolved in an introductory White Paper. We have chosen the following series of interrelated topics to highlight some of the most important issues and considerations for modern public safety agencies. As a Systems Integrator with 30 years of experience and expertise in the specific area of delivering mission-critical solutions to the most demanding customers, Sigma Wireless is well placed to answer any further questions you might have and work together with you to design the very best solution to fit your future operational requirements.

4.1 Legal framework

Governments across Europe and around the world have an obligation to provide reliable, timely public safety services to their citizens, which in turn require a robust, constantly updated legal framework. Historical, geographical, political, social, economic & environmental conditions may have led to different structures, processes and procedures being implemented from country to country, but the challenges of legislating and regulating such foundational services are similar across all jurisdictions, especially when we take into account the need for cross-border and international cooperation to fight crime, terrorism and natural disasters in a time of social and political tensions and climate change.

One of the most important and basic issues to be agreed and legislated for is who will actually own, build, operate and maintain public safety networks over the long term. Networks can be owned by the Government or public safety entity, a specialised or commercial network operator, some combination of both or even agreed third parties. If a public entity does not actually own the network, strict provisions must be made to guarantee its continued operation in case private owners run into financial difficulties or decide to sell all or part of the network to potentially hostile actors.

There are multiple legal issues which will need to be debated prior to setting up a next generation, public safety mobile broadband network, regardless of ownership of key network assets such as core and RAN, and availability of dedicated spectrum including:

National roaming: the Governments of Finland, Norway and Australia are all mandating national roaming so that access can be gained by public safety users to multiple mobile operators' networks to increase coverage, resilience and redundancy. Existing contractual agreements and operator consent might be required, so this must be considered when setting timelines, deadlines etc. for important milestones during migration from legacy solutions.

Priority access: National laws may need to be modified to allow public safety users to gain priority access to mobile networks not dedicated to first responders. In the case of some countries, net neutrality rules may need to be adjusted for emergency services personnel to gain access to critical data during major incidents.

Fairness for all network operators: If public safety agencies need to subsidise specific network operators to provide extended area coverage, hardened assets etc., competition laws and potential objections by other mobile operators need to be considered to avoid lengthy legal delays.

Once contracts are signed, penalties for non-compliance need to be clear, proportionate and enforceable, so it is important for Governments and public safety agencies to build strong, trusted, open relationships with all potential suppliers from the start of the process.

Other considerations will include very clear provisions for who pays for what before, during

and after the process of implementing the solution; sufficient provisions for safeguarding users during the migration from existing systems to the new system; the viability of different business and operational models (see 4.4 below) and the actual length of contracts: a long contract offers stability and guarantees to suppliers, but could potentially tie the user organisation into a solution for longer than desired if changes are needed; a shorter contract provides instability if no extensions are considered based on certain performance criteria being achieved.

Finally new services being introduced as 3GPP standards and solutions are implemented such as 5G-enabled cameras, drones, facial recognition and precise location may require new laws or regulations to be passed, perhaps with the agreement of or negotiations taking place with human rights and privacy advocacy groups.

4.2 Technological convergence

Having dedicated a whole section of the previous chapter to 3GPP, there is no need here to repeat its importance in the ongoing development of a comprehensive technological solution for the next generation of mission-critical networks, starting with 4G/LTE and continuing with 5G and beyond. The global public safety community is working closely with other similar-minded mission-critical communities to add all required additional services to core 3GPP offerings. Necessary protocols and interfaces are being put in place to allow trusted non-3GPP solutions - including TETRA - to interact, interwork and converge with 3GPP systems as advanced IT and OT (operational technology) networks are incorporated within the overall 3GPP framework to create powerful end-to-end solutions which will transform enterprises, industries, economies and societies.

To take full advantage of the enormous opportunities presented within the 3GPP framework, public safety agencies must have a clear idea of the most appropriate base station architecture, transmission network, core network architecture and service and support platforms that best fit their requirements (also see 4.4). Due to the flexibility and versatility of multiple hybrid solutions for deploying communications equipment, devices and services across wide areas for public safety agencies, control rooms, related critical users, as well as vulnerable members of the public, it is critical for all possible options to be compared and assessed. When commercial mobile operators and their networks are commissioned for full or partial radio access for first responders, even more checks will need to be made and guarantees given.

Compared to the relatively inflexible, best-effort, vendor-driven and operator-driven earlier generations of commercial cellular technology, LTE Advanced and 5G solutions have been designed from the start to deal with the rigours of 2020s mission-critical solutions such as those now being deployed by public safety. Significant work on global standards have enabled neutral host deployments, private networks, small cells, edge computing, massive IoT and low-latency communications. Combined with software-defined networking (SDN), network functions virtualisation (NFV) and cloud-native methodologies, public safety

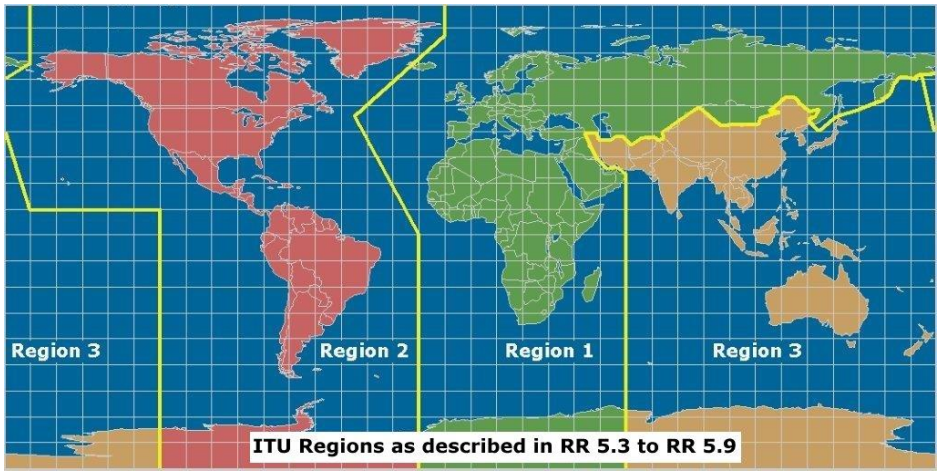
agencies and related mission-critical verticals now have powerful tools allowing them greater control and visibility of network operations.

However, building a nationwide public safety network is a very different challenge to building a private network for a single or small number of industrial sites. Depending on the geography and topography of the coverage area, there may be significant variations in the configuration and requirements of urban, suburban and rural sites, requiring close attention. Incorporating resilience and redundancy, i.e. no single point of failure, combined with as close to 100% availability as possible and all necessary security measures across all network layers and domains is no easy task, requiring Governments and agencies to choose trusted, competent, experienced partners for design, deployment and operations. Even as modern networks become more open and modular, it remains important to keep everything as standardised and future-proof as possible, avoiding expensive lock-ins.

Government and public agencies must also be aware that most mobile operators currently use WiFi to provide indoor solutions. Wi-Fi cannot guarantee the same level of availability, security and resiliency of 3GPP-compliant technologies so alternative solutions will need to be developed for mission-critical networks. Fortunately, 3GPP, working together with other industry bodies, have developed such solutions. There can be no compromises at any stage of the process when delivering public safety communications. Technological solutions are now available to allow us to move to the next stage in our journey with confidence, but these solutions need to be tailored to the real operational needs of agencies.

4.3 Spectrum

Spectrum is the lifeblood of all telecommunications services, graphically visualised in the colourful and comprehensive Frequency Allocation Tables produced and updated on a regular basis by the ITU with the assistance of regional and national frequency regulators and experts in attendance and ratified at World Radiocommunication Conferences held every 4 years.



Source: ITU

Low frequency (LF) and Medium frequency (MF) Bands

Band [kHz]	Region 1	Region 2	Region 3
148.5-283.5	A[1]	NA	NA
525-526.5	NA	A	NA
526.5-535	A[1]	A	A[1]
535-1605	A[1]	A[2]	A[1]
1605-1606.5	A[1]	A[3]	A[1]
1605.5-1705	NA	A[3]	NA

- [1] - Subject to GE75 Agreement (LF/MF Broadcasting)
- [2] - Subject to RJ81 Agreement (MF Broadcasting)
- [3] - Subject to RJ88 Agreement (MF Broadcasting)

High Frequency (HF) Bands for national broadcasting

Band [kHz]	Region 1	Region 2	Region 3
2300-2495	A[4]	A[4]	A[4]
2495-2498	A[4]	NA	NA
3200-3400	A[4]	A[4]	A[4]
3900-3950	NA	NA	A
3950-4000	A	NA	A
4750-4995	A[4]	A[4]	A[4]
5005-5060	A[4]	A[4]	A[4]

- [4] - Only in the "Tropical Zone" (RR 5.16 to RR 5.20 and RR 23.3 to RR 23.10)

High Frequency (HF) Bands for international broadcasting under RR12

Band [kHz]	Region 1	Region 2	Region 3
5900-6200	A	A	A
7200-7300	A	NA	A
7300-7400	A	A	A
7400-7450	A	NA	A
9400-9900	A	A	A
11600-12100	A	A	A
13570-13870	A	A	A
15100-15800	A	A	A
17480-17900	A	A	A
18900-19020	A	A	A
21450-21850	A	A	A
25670-26100	A	A	A

Very High frequency (VHF) Bands

Band [MHz]	Region 1	Region 2	Region 3
47-50	A[5]	NA	A
50-54	A[5]	NA	NA
54-68	A[5]	A	A
76-87	NA	A	NA
87-87.5	NA	A	A
87.5-108	A[5,6]	A	A
162-174	A[5]	A	A
174-216	A[7]	A	A
216-230	A[7]	NA	A

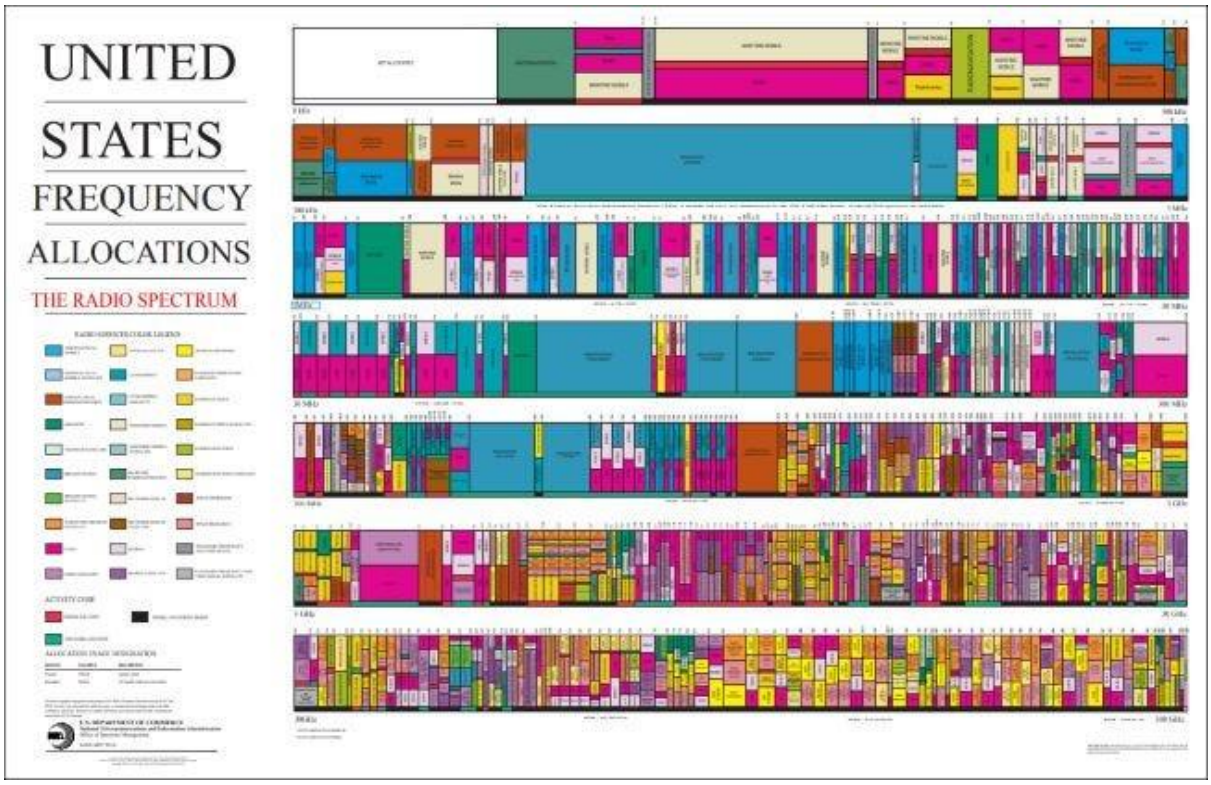
- [5] - Subject to ST61 (Rev.2006) Agreement (Analog TV and Sound Broadcasting) or GE89 (Rev. 2006) Agreement (Analog TV)
- [6] - Subject to GE84 Agreement (VHF Sound Broadcasting)
- [7] - Subject to GE06 Agreement

Ultra High frequency (UHF) Bands

Band [MHz]	Region 1	Region 2	Region 3
470-862	A [8]	A	A
862-890	A [9]	A	A
890-960	A [9]	NA	A

- [8] - Subject to GE06 Agreement
- [9] - Only in some parts of African Broadcasting Area (See RR 5.322)

Source: ITU



Without sufficient, appropriate spectrum being made available, it is clear that Governments and public safety agencies would be unable to perform their regular and emergency duties in support of the public. However, their requirements are often pitted against those of commercial network operators, service providers and other social and economic actors, as

the most valuable tranches of radio frequencies are regularly auctioned off for billions of dollars across European, American and Asian markets.

In the early days of wireless, when public safety communications services were restricted to broadcast and group voice calls and status messages, a handful of narrowband frequencies in VHF for wide area and UHF for extra capacity in more congested cities were sufficient. Even when most European nations switched to nationwide TETRA networks, 2 x 1-2 MHz in the NATO 380-400 MHz UHF band for constellations of base stations operating a handful of 25 kHz TDMA V+D channels was deemed sufficient to cater for perhaps tens or at most hundreds of thousands of first responders, even in the largest countries. Once real-time video, connected cars, drones and robots are added to the mix during 2020s and 2030s, it becomes obvious that public safety agencies will require dedicated and/or priority access to significant amounts of spectrum across multiple bands.

Although both GSM and TETRA standards began development at roughly the same time within ETSI during the late 1980s/early 1990s, commercial interests drove GSM to a billion global subscribers and beyond within a decade, leading to 3GPP's creation to develop mobile wideband and broadband solutions, hundreds of billions of dollars spent in expensive auctions and the advent of the smartphone that required even greater data rates, services and 4G/LTE standards. Attempts were made by the TETRA community to develop wider data channels (TEDS), but it became clear during early 2010s that our community would need to engage with 3GPP to develop fully-functional, affordable, future-proof, next-generation solutions on a global scale.

Spectrum for mobile broadband services has tended to be awarded to commercial mobile operators at auction for significant amounts of money. Non-3GPP solutions such as WiFi and Bluetooth have reached economies of scale taking advantage of unlicensed spectrum, but lack the required security, availability, range and number of interference-free subscribers required by mission-critical users. Shared spectrum options are becoming available for enterprise users operating in well-defined areas. First responders use a wide range of solutions, including commercial networks, for offloading non-mission-critical traffic, but dedicated spectrum is the only guaranteed means of providing full mission-critical service under all circumstances.

In the early days of the public safety community's participation in 3GPP, the goal was to secure at least 2 x 10 MHz of prime spectrum in the prime 700 MHz band (FDD Band 28) which was being freed up by a more efficient use of TV broadcast signals. In the majority of cases, the main 2x30 MHz tranche has been auctioned off to European mobile operators as a 5G coverage layer. 2x5 MHz and 2x3 MHz at either end of the main B28/n28 band is still available for public safety services.

3GPP has also standardised multiple options within the common 400 MHz UHF bands (B31/72 in 450 MHz and B87/88 in 410 MHz in Europe), with one option leading to public safety sharing spectrum with other key sectors such as utilities, transport etc. to build nationwide wide-area networks capable of satisfying current and future requirements. If

sufficient spectrum is available for public safety in the recognised 3GPP bands in 410 MHz (especially Band 88) and 450 MHz (Band 31 or 72), then these should be carefully studied and prioritised as guaranteeing broadband services over a similar coverage area to existing TETRA narrowband service.

As we move forward into the brave new world of 5G and beyond, and as public safety agencies inevitably look to incorporate totally new services such as autonomous vehicles, real-time video/mixed reality, robotics, advanced analytics etc. into their common operational procedures, mid-band and higher-band (mmW, THz etc.) spectrum will need to be made available in a timely manner as it can require a full decade or more of preparation to deliver harmonised spectrum.

European Commission is currently consulting on offering a significant part of n77 (3.8-4.2 GHz) for private 5G networks, immediately above the current lucrative and harmonised 5G mid-band n78 spectrum. As more research and field tests are conducted into massive MIMO, beamforming and other innovative active antenna technologies, the possibility opens up in the medium-term for massive amounts of data to be transferred over shorter distances for both indoor and outdoor use at hotspots, including vehicles, police stations and major incidents.

4.4 Network architecture and models

It should be clear to the reader by now that all the hard work carried out within 3GPP by the global telecommunications community together with the critical communications community and other standards, specifications, public and private industry bodies over the past decade is paving the way for radical new approaches to designing, building and implementing mission-critical solutions. In fact, as far as the technology itself is concerned, most of the building blocks for these new solutions have already been developed. It is now time for equipment suppliers, software developers, service providers, systems integrators, industry experts and critical end-users to finally deliver on the promise and turn erstwhile technological laggards into digital transformation leaders.

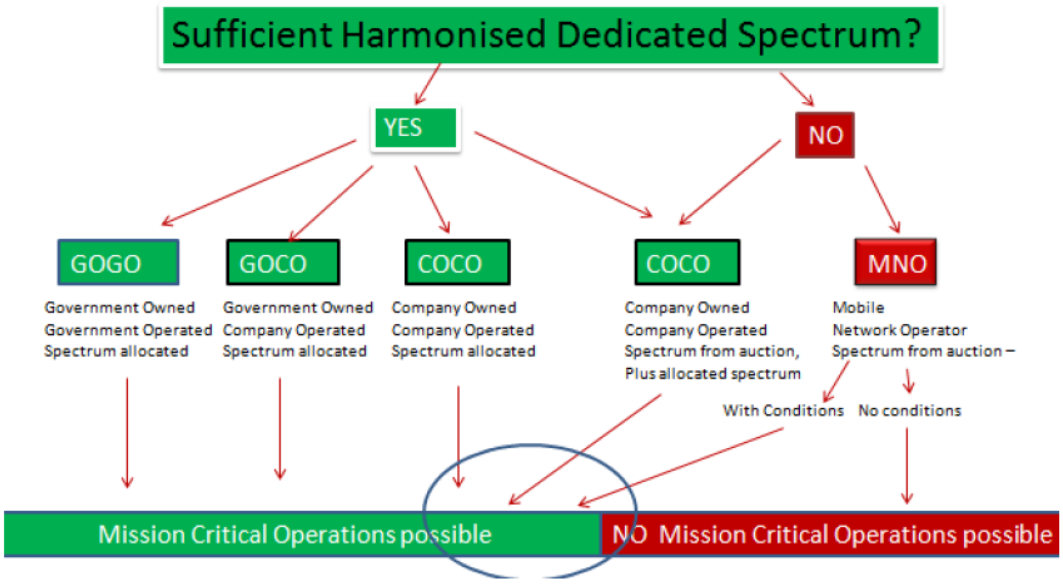
As mentioned during Chapter 3, the increasing demands of modern citizens and enterprises have been driving exciting new network architectures, with many of the more innovative approaches adapted and adopted from the IT, cloud and data centre world of hyperscalers, OTT players and global service providers.

Virtualisation, software-defined networking, and the move towards cloud-native and eventually serverless is driving the whole communications industry away from traditional, inflexible, outdated structures towards the service-centric, fast-moving, reconfigurable full 5G and beyond approach that will be required for suppliers, operators, integrators and users to survive and thrive in the 2020s/2030s continuous integration/development/testing DevSecOps environment. Public safety and other mission-critical thought leaders must be aware of this process so that they can maximise the benefits while minimising the massive

potential downsides of moving too fast and perhaps breaking things that cannot afford to be broken. Everything must be secured, managed, orchestrated and automated to cope with the pressures of modern emergency response.

Unfortunately, during late 2021, no single, optimal model has been agreed for the next generation of nationwide public safety broadband networks. The traditional, fully dedicated, fully owned, self-built, CAPEX-heavy network is the most expensive, but also the only one that offers public safety agencies complete control. OPEX-heavy commercial networks without additional legislation nor priority provisions are the cheapest solutions and the fastest – in theory – to implement, but totally unacceptable because of the enormous liabilities of moving away from a secure, robust TETRA network to a best-effort commercial one for essential, life-or-death communications.

This leaves an almost infinite number of permutations for hybrid solutions to be implemented by those pioneer countries and agencies detailed in Chapter 3, as well as all those countries and agencies currently in the process of procuring such solutions. They must try to keep costs down while guaranteeing high service levels, continued innovation and the fast turnaround of new services. They will almost certainly require their own dedicated core, sufficient dedicated spectrum for core and specialised coverage and services as well as priority access to other networks, commercial and private, as well as extended area coverage and a wide range of traditional devices such as smartphones, tablets, dispatcher and control room equipment, as well as a new generation of edge devices adapted to the very specific requirements of first responders.



Source: TCCA Models for building and operating BB-PPDR network.

Regardless of the final network architecture and model chosen by individual countries and public safety agencies, the importance of the work of the past decade must not be

underestimated. A full toolkit of services and applications, enabled by a growing ecosystem of network equipment and device manufacturers, systems integrators and solutions providers are being verified and standardised by a global community, opening up new opportunities that must be explored, adopted and continuously integrated, developed and improved together with the end-users themselves. New generations of first responders will discover new ways of working that can be shared quickly and effectively with a more open, collaborative, global community.

4.5 Services

Regardless of the underlying technology, spectrum bands or network design finally chosen by public safety agencies, what ultimately counts for end-users during their daily operations and high-tension emergency situations are the services and applications that run over the network. For first responders, the quality, predictability, ease-of-use and guaranteed availability of these services could literally be the difference between life or death.

Any new network - regardless of increased bandwidth, higher speeds and lower latency - must be able to deliver all the essential, tried-and-tested services currently provided by narrowband TETRA and Tetrapol networks. The best example from current and age-old public safety practices are the near-instantaneous high-quality voice group calls involving potentially hundreds of officers across multiple cells that are a given and non-negotiable. Until such basic, reliable voice and short data services can be provided by any new network, existing networks will need to be maintained, at considerable cost and with the added complexity that diverse services must be delivered efficiently over multiple access and core networks.

Over the past two decades, TETRA networks have also provided a wide range of added-value services running natively over narrowband voice and control channels or managed by dispatchers in increasingly sophisticated control rooms. Status messaging, short data service (SDS), limited packet data, late entry, ambience listening, dynamic re-grouping etc. have become embedded in existing practices and procedures, requiring 3GPP SA6 members to make sure these are either replicated over later version 3GPP networks or some new, equivalent solution to the existing one can be found.

In particular, the basic, key device-to-device aka Direct Mode (DMO) service allowing off-network communications to take place directly during certain localised operations has provided particularly challenging for the 3GPP community because of the use of lower power devices and the lack of incentives for commercial operators to offer such services. Lower-power ProSe (Proximity Services) has been developed as a work-around, with close cooperation with the automotive community also providing a direct PC5 interface that could be part of a longer-term solution. Isolated E-UTRAN Operation for Public Safety (IOPS) is another creative solution developed within 3GPP to allow selected base stations to continue operating when the link to core network fails.

Whereas basic mission-critical services (MCX in 3GPP-speak) have always been baked into legacy PMR networks such as TETRA and Tetrapol, these same services have been implemented at the application layer in 3GPP systems requiring LTE and future 5G networks to be hardened and optimised to guarantee end-to-end service KPIs.

Fortunately, each 3GPP release builds upon the previous one and market forces lead to continuous improvements to the underlying network, so as more public safety and mission-critical users adopt 3GPP solutions, the more robust and responsive they become. Priority and pre-emption as part of a larger overall Quality of Service and policy enforcement framework within 3GPP networks, together with new 5G features such as network slicing and URLLC (Ultra-Reliable Low Latency Communications) enable an even wider range of advanced services for mission-critical users.

3GPP SA6 has also worked on a common API framework (CAPIF) that allows verticals such as public safety to incorporate third party applications in a standardised and secure manner into their operations. This modern approach to services and operations within 5G and beyond networks should allow more advanced services to be shared across the mission-critical community with public safety working together with railways, industry 4.0, automotive sector and others to build common applications that can be automated and orchestrated to build comprehensive, multi-sector smart cities, communities and nation solutions underpinned by enhanced, integrated, native public safety solutions. Although we may be several years away from achieving such lofty goals, the roadmap is becoming clearer by the day.

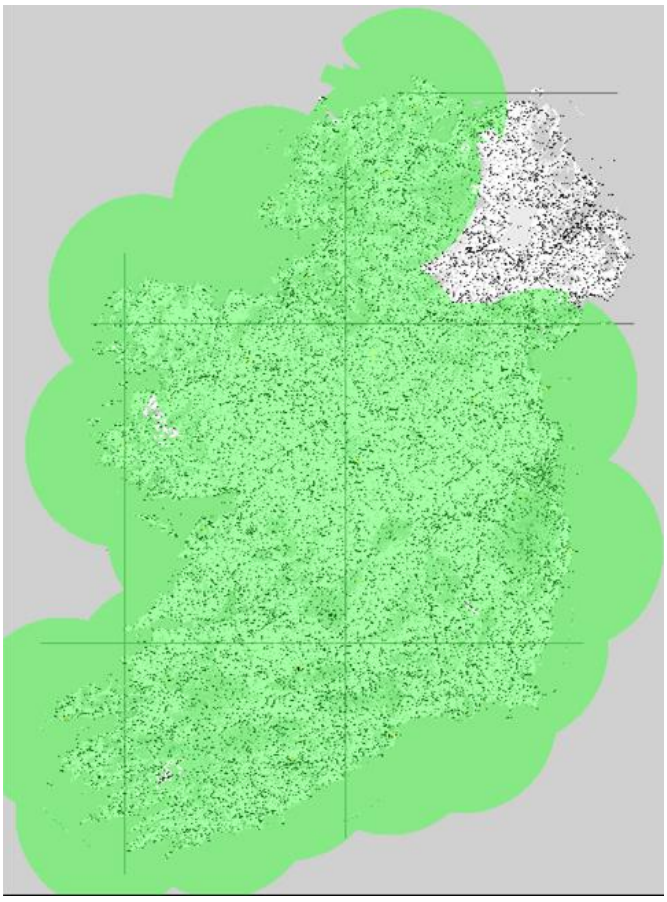
4.6 Full Coverage

Perhaps the most important metric of all for public safety communications is the level of radio coverage achieved by the base stations deployed across the network. Any coverage gaps in a public safety network could have disastrous consequences during an incident, if first responders are unable to communicate with each other or back to command-and-control posts.

Commercial mobile network operators tend to report network coverage by focusing on the percentage of the population with regular radio access, thereby emphasizing network build-out in major towns and cities, roads, transport hubs, stadiums and other tourist attractions. However, 95-98% population coverage might be as low as 50-60% geographical coverage – or even lower – in those countries with significant rural and remote areas, which is totally unacceptable for public safety organisations that need to respond to all incidents in a timely fashion, wherever they occur.

Public safety network coverage has therefore always been measured by geographical coverage, with figures as high as 98-99% being common across Europe, as well as reaching at least 20 km out to sea as well as covering national air-space. To achieve this, TETRA networks operate at lower UHF frequencies (380-400 MHz), thereby requiring an order of

magnitude fewer base stations than a mobile network operating around 2 GHz. There also tend to be several orders of magnitude fewer users on a public safety network than on a commercial network, and these users tend to use PTT group call services which are shorter than private calls and only occupy one voice channel per cell.



Source: Sigma Wireless TETRA Ireland coverage map

As mentioned in section 4.3 above, sufficient public safety spectrum in the recognised 3GPP bands of 410 MHz (especially Band 88) and 450 MHz (Band 31 or 72), must be prioritised as guaranteeing broadband services over a similar coverage area to existing TETRA narrowband service, as well as starting to study future use of the NATO 380-400 MHz band beyond 2025/30 as services are migrated from TETRA to 3GPP services.

It is therefore obvious that extra measures will be required to cover extensive parts of nations that have previously not had cellular coverage in previous generations of mobile technology. Driven by mobile operators in countries with vast rural areas such as Australia, America, Brazil etc., 3GPP continues to push the boundaries to extend coverage of LTE and future 5G. Tunnels, metros, valleys and other remote geographical areas etc. also need to be covered, with more creative network sharing and neutral host deployments – as well as more advanced satellite/non-terrestrial solutions – becoming fully integrated into 3GPP-based mobile and more specialised operators and systems integrators' tool-kits.

As industry 4.0 heavyweights also contribute more to standards and as mission-critical users understand the multiple limitations of Wi-Fi solutions, indoor coverage is also taking centre stage, with better coordination between small cells, more intelligent antenna solutions and more precise positioning. Again, more open and flexible mobile RAN and core solutions allow latest generation mobile networks to become more distributed and disaggregated at the edge, improving signal strength, extending coverage to previously difficult-to-reach places and thereby improving the user experience for more demanding mission-critical users.

Reaching the same level of coverage as existing TETRA networks is extremely challenging and potentially very costly. However, as the range of services required by first responders increases to include more intensive use of data and real-time video, the emphasis switches from achieving basic coverage to providing sufficient capacity at the cell-site and cell edge to provide such services. Transportable base stations have become a solution for coverage and additional capacity for both planned and unplanned events, with tactical bubbles, relays, vehicle repeaters and airborne coverage solutions such as UAVs and HAPS all being studied and implemented.

Working more closely than ever with other similar-minded mission-critical users from multiple vertical sectors and collaborating with the full ecosystem of regulators, equipment suppliers, solutions providers, network operators, systems integrators and industry experts, the public safety community is finding new, innovative ways of guaranteeing sufficient coverage and capacity for daily operations and emergency situations. There has been significant progress on all fronts in recent years, so as more countries and agencies roll out standards-compliant mission-critical services across the globe, the sharing of information and experience of best practices is leading to a wider range of solutions to perennial industry challenges. Coverage is also closely tied to robustness, resilience and network availability, which is treated briefly in the next section.

4.7 Full Service Availability

It should be becoming clear now that building a next-generation public safety broadband network fit for the 2020s is no easy task, but that the modern tools required to build it are now becoming available thanks to an enormous collective effort of a flourishing, fully engaged and committed global community working within 3GPP and other global institutions and organisations. Whereas all the above items and requirements such as technology, spectrum, network architecture, services, coverage and capacity are all vitally important, full service availability is the one SLA or KPI that really counts. If all the above have been taken into account, but the service is not actually available when it is needed most, then the network(s) and services cannot be considered truly public-safety or mission-critical grade.

In the critical communications world, the full robustness, redundancy and resilience of all hardware and software network elements must be guaranteed in all locations at all times,

whatever the cost. In the public safety world, there are no trade-offs and no compromises. Public safety operators require a full mapping of all assets, with full control over physical assets, network equipment, radio sites, buildings, cables, including control room positions, dispatchers, NG112 solutions.

Regardless of the technology being used: TETRA today, LTE/5G tomorrow, public safety networks must continue to work when all other networks fail, i.e., in emergency situations such as natural disasters, floods, terrorist attacks that destroy significant parts of critical national infrastructure and damage key network components.

Backhaul redundancy, back-up power, perhaps for several days in some sites, including diesel generators or more environmentally friendly solar panels and full risk assessments, including climate change, terrorism and social unrest, human error, acts of God, are all part of the PPDR mindset that prepares for worst-case scenarios and thinks through automatic procedures to minimise the consequences of certain actions and incidents.

As we move into a 5G world, some of the challenges of achieving full service availability can be solved, while new ones will arise. Such is the nature of a dynamic radiocommunications environment. Critical data at rest and in transit needs to be protected. Private, public, hybrid and multiple cloud configurations require close collaboration between Governments, agencies, industries and enterprises. Operational support systems and databases need to continue to function; regular maintenance tasks need to be programmed to avoid network down-time or outages.

Finally, any discussion regarding full service availability naturally turns to security issues, including physical security, cybersecurity and trust regimes including confidentiality, integrity as well as availability.

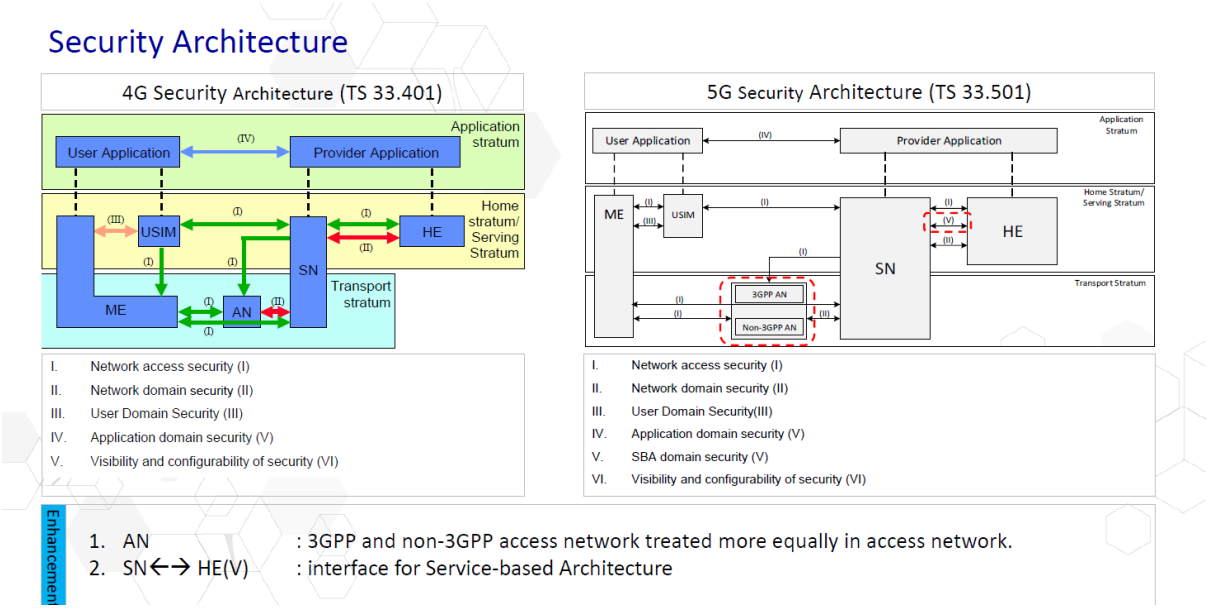
4.8 Security Aspects

Securing the networks of today and tomorrow requires new tools. Self-contained TETRA and Tetrapol networks dedicated to first responders and their support systems, designed with security in mind from the start, have served their users, Governments and societies well for the past fifteen to twenty years, and will continue to do so during 2020s if and as required. But modern public safety networks can no longer provide only voice communications with a little bit of data. As we move to next-generation solutions, we can no longer entirely rely on completely isolated networks with trusted users. New approaches to security are required to cope with the massive amounts of critical data, video and multimedia to be transferred from device to device across vulnerable networks.

Secure communications has been at the heart of TETRA network standardisation and development since Day 1. As soon as NATO awarded dedicated spectrum for future European nationwide public safety networks in 380-400 MHz back in mid-1990s, radio experts from Government departments working together with TCCA within a special working group, SFPG (Security and Fraud Protection Group) and Working Group 6 within

ETSI TETRA/TCCE have produced numerous technical documents detailing how to keep TETRA networks secure. The TETRA standard includes mutual authentication, where the network authenticates the mobile terminals and the terminals check the network; air interface encryption if a given and options are available for agencies to add end-to-end encryption. Similar measures have been adopted by Tetrapol and P25 networks.

3GPP also has a specific group dedicated to all security aspects of its specifications: SA Working Group 3 (SA3), which produces comprehensive security assessments in Series 33 documents: TS 33.102 for 3G; 33.401/2 for 4G and 33.501 for 5G. As with TETRA, 3GPP solutions are inherently secure due to the SIM (Subscriber Identity Module) card introduced in GSM. Various authentication, identity and encryption methods are enforced at the different network layers with each release of 3GPP technology updating and building upon the security requirements of the previous one.



Source: 3GPP

The public safety community has been involved in 3GPP security since LTE, suggesting and working together with the wider community on new measures to secure assets of increasing value, critical national infrastructure, critical data, taking into account and managing network complexity, longer supply chains, a greater number of interfaces and third-party applications.

New zero trust methodologies with role-based access controls, security by design, DevSecOps CI/CD pipelines, segmentation and isolation of separate network domains and all north-south and east-west traffic, provide added safeguards to operators and users within increasingly software-defined networks, while recognising that no modern communications network can be 100% secure. It is important for attack surfaces to be minimised and access to valuable data only made available to trusted and verifiable users, with greater

automation and visibility allowing management systems to monitor any suspicious behaviour.

5G has been designed for an infinite number of use cases stretching way beyond the mobile broadband focus of original 4G/LTE networks. AR/VR/Mixed Reality headsets, drones, autonomous vehicles, untethered factory robots, sophisticated early warning systems and other smart city applications require 5G systems to respond to threats automatically, without human intervention, within microseconds, with the ability to self-heal and self-reconfigure as circumstances change. These systems must be secure by design and hyper-aware of their environment.

Finally, due to the increased value and importance of 5G systems, Government authorities are taking a closer look at complex, global supply chains, restricting or banning High Risk Vendors (HRVs) from supplying key network components such as radio access, core or management systems. Such measures may be justified to protect key assets, but it is also acknowledged that they may lead to fewer choices for network operators and public safety users, higher costs and potentially inferior technical solutions if companies with more advanced solutions find themselves blacklisted.

4.9 System Affordability

All of the above must be fully accounted for, funded and paid for by the relevant Government and public safety authorities out of general taxation, Government borrowing or some other creative form of finance. The move towards more standards-based, commercial-off-the-shelf (COTS) solutions with as few proprietary, customised features as possible and a more competitive procurement environment should make it slightly easier for departments to keep to budget.

However, many of the additional requirements laid out above that go beyond the normal boundaries of commercial deployments will inevitably lead to rising costs in certain areas. Well designed and well-defined public-private partnerships offer one solution; sharing costs with other critical sectors such as utilities, transport, major industries is another. Unfortunately, as history has shown us on many occasions, the final cost of not providing adequate public safety communications when something goes badly wrong can be very, very high indeed.

One of the most important lessons we have learned in recent times from our participation within 3GPP is the critical nature of global standards for the provision of affordable solutions to public entities working on limited budgets. The opening up of network interfaces within radio access and core networks is the beginning of a long process, which should lead to greater choice, greater innovation in new mission-critical services, and lower costs as public safety agencies work together with innovative new suppliers to develop the special applications required by their users. The availability of 3GPP network equipment, devices and applications at lower frequencies such as 400 MHz and 700 MHz will also ease the

migration from legacy networks to new ones, with greater automation, control and visibility reducing the cost of management systems.

Perhaps the greatest challenge for public safety agencies over coming years will be managing the migration and replacement of existing narrowband networks towards new 3GPP-based solutions. The experience of the UK Home Office's Emergency Services Network (ESN) has shown how costly it can be to have to fund and operate two separate networks over an extended period of time. USA's FirstNet has tried to manage this situation by separating mission-critical voice communications (which currently continues to run mainly over P25 networks) and high-speed data/video which can only realistically be run over AT&T's FirstNet network.

It will be interesting to watch what happens in Finland with VIRVE 2.0 and France with RRF/ACMOSS between now and 2024-5 to see how successful they are in delivering a fully-functional nationwide public safety broadband solution that is a mix of dedicated frequencies, tactical bubbles, and dedicated cores connected to mobile operators' radio access networks. Some European countries will insist on having access to dedicated spectrum as the only means to guarantee service levels when disaster strikes. Whichever model public safety agencies finally choose, it is important for them to take advice from and work together with companies and individuals who really understand how to design, build and operate mission-critical grade networks and services.

5 The way forward

Hopefully we have given you a good overview of the current state and future potential of public safety communications as we move from highly secure, robust narrowband technologies such as TETRA to a mission-critical services framework embedded within the much larger and diverse global 3GPP community. We have looked at some of the major issues that need to be considered and dealt with as we move from one generation to the next, including many of the challenges and opportunities of embracing new ways of working and a new mindset for a new era.

Migration is now well under way and will only accelerate over the next 3-5 years, so for all those Governments and agencies who are still waiting to see what happens, the time to prepare for the future is now. You need to start engaging with all those agencies, companies and individuals within our community who have the experience and expertise to take a look at the path you wish to take and make sure you make the right steps along the way.

We live in interesting times, facing the unprecedented challenges of climate change, social upheaval, terrorist threats, cyber warfare and online radicalisation and misinformation, all increasing the threat of natural and man-made disasters. When it comes to public safety communications, we must make sure we protect and guarantee existing levels of service, while at the same time thinking outside the box, staying at least one step ahead of adversaries and preparing for worst-case scenarios. We cannot accept the status quo. We must strive for new, improved models to deal with the new reality of life in the 2020s and

2030s.

Sigma Wireless are celebrating 30 years of continued, valuable service to public safety and mission-critical users in their native Ireland and globally. The author wrote his first TETRA report back in 1996 and is now an active member of 3GPP, ETSI and TCCA. We look forward to serving the public safety community for many, many more years to come. Please get in touch with us if you would like to know more about any of the topics discussed in this White Paper or if you would like us to help you take the next steps on your own critical communications journey.

September 2021.

Peter Clemons – Founder, QUIXOTICITY-EU

Peter Clemons has been involved in the global critical communications industry for 25 years. Peter is a former Director & Board Member, TCCA, who has worked closely together with all key industry & community players to promote critical communications technology standards across the world. Peter is Founder & Managing Director of France-based consulting firm, Quixoticity-EU - founded as UK-based Quixoticity Ltd back in 2012 - member of ETSI, 3GPP, TCCA & Founding Member, EUWENA. He now spends most of his time studying, developing & implementing secure, end-to-end, mission-critical LTE/5G solutions, having moved to France during 2020.

Sigma Wireless Communications

Sigma Wireless is a fully Irish owned independent systems integrator, providing Mission Critical Communications since 1991 in Ireland and Internationally Our expertise focusses on the provision of solutions and support services for the **critical communications systems** utilised by our customers to meet the strict operational and safety criteria requirements as set by each market sector

Sigma Wireless is a founding partner of TETRA Ireland, the only nationwide 400 MHz nationwide network in Ireland. We were responsible for the designed and build of this network and have supported it for over 12 years. This network is by far the most resilient Mission Critical Network in Ireland and delivers 99% land mass coverage and has delivered end to end performance of 99.995% throughout that period. We provide 24x7x365 support to TETRA Ireland and all our customers in Ireland.

We have designed, built, and continue to support systems and solution in over 20 countries world-wide.

Sigma Wireless is a Motorola Platinum partner, Nokia Preferred Partner and has relationships with many of the worlds biggest providers in the critical communications sector including Rohde and Schwarz, Frequentis, Jotron, Reveal, Satel and Radwin to name but a few.

Sigma Wireless prides itself on being a leader in innovative technologies. We have always embraced and lead in emerging sectors, from having the first RET Tetra antennas to driving the way in Private LTE. Sigma Wireless is a founding member of EUWENA.

6 Glossary

3GPP	Third Generation Partnership Project
4G	Fourth Generation of Mobile Technology
5G	Fifth Generation of Mobile Technology
5G-ACIA	5G Alliance for Connected Industries and Automation
5G IA	5G Infrastructure Association
AI/ML	Artificial Intelligence/Machine Learning
AR/VR	Augmented Reality/Virtual Reality
ARIB	Association of Radio Industries and Businesses (Japan)
ATIS	Alliance for Telecommunications Industry Solutions (USA)
CAPEX	Capital Expenditure
CBRS	Citizens Broadband Radio Service (USA)
CCSA	China Communications Standards Association (China)
CI/CD	Continuous Integration/Continuous Development/Delivery
EUWENA	European Users Wireless Enterprise Network Association.
ETSI	European Telecommunications Standards Institute
FDD	Frequency-Division Duplex
FDMA	Frequency Division Multiple Access
GSM	Global System for Mobile Communications (2G Technology)
HAPS	High Altitude Platform Stations
HRV	High-Risk Vendors
HTTPS	Hypertext Transfer Protocol Secure
ITU	International Telecommunication Union
IWF	Interworking Function

KPI	Key Performance Indicators
LMR	Land Mobile Radio
LTE	Long-Term Evolution (4G Technology)
MCPTT	Mission-Critical Push-To-Talk
MCX	Mission-Critical Services (PTT, Data, Video)
MEC	Multi-Access Edge Computing
MIMO	Multiple-Input, Multiple-Output
mmW	Millimetre Wave
NATO	North Atlantic Treaty Organisation
OMA	Open Mobile Alliance
OPEX	Operation
OTT	Over The Top
P25	APCO Project 25
PoC	Push-to-talk over Cellular
SLA	Service Level Agreement
TCCA	The Critical Communications Association
TDD	Time-Division Duplex
TDMA	Time Division Multiple Access
TEDS	TETRA Enhanced Data Services
TETRA	Terrestrial Trunked Radio
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association (South Korea)
TTC	Telecommunication Technology Committee (Japan)
UAV	Unmanned Aerial Vehicle

UMTS	Universal Mobile Telecommunications System (3G Technology)