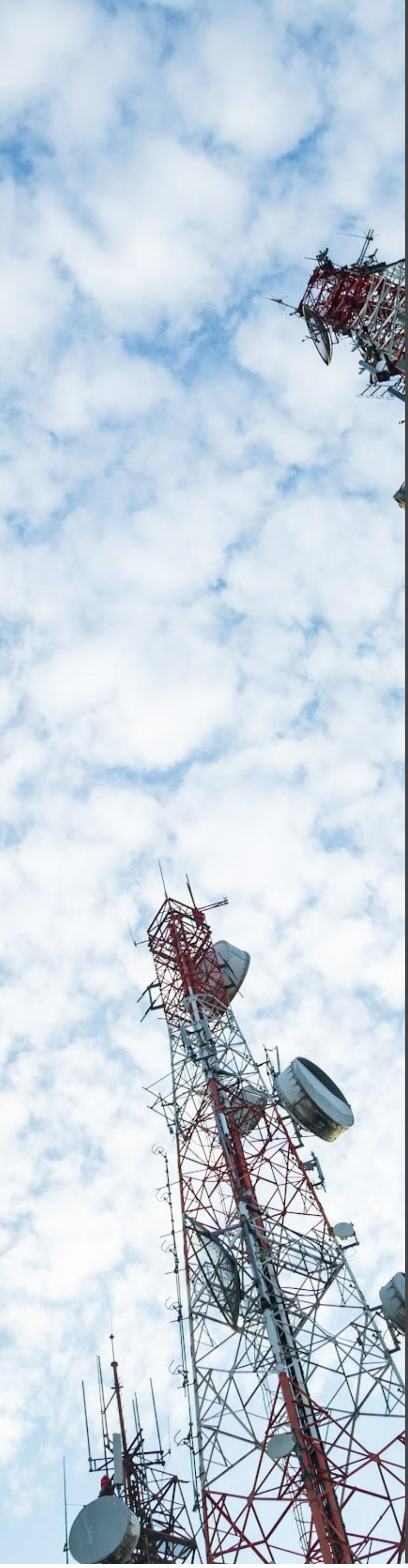
Navigating the chasm

The shortest critical path to Next-Generation **Public Safety Networks**

pwc

www.pwc.com/me



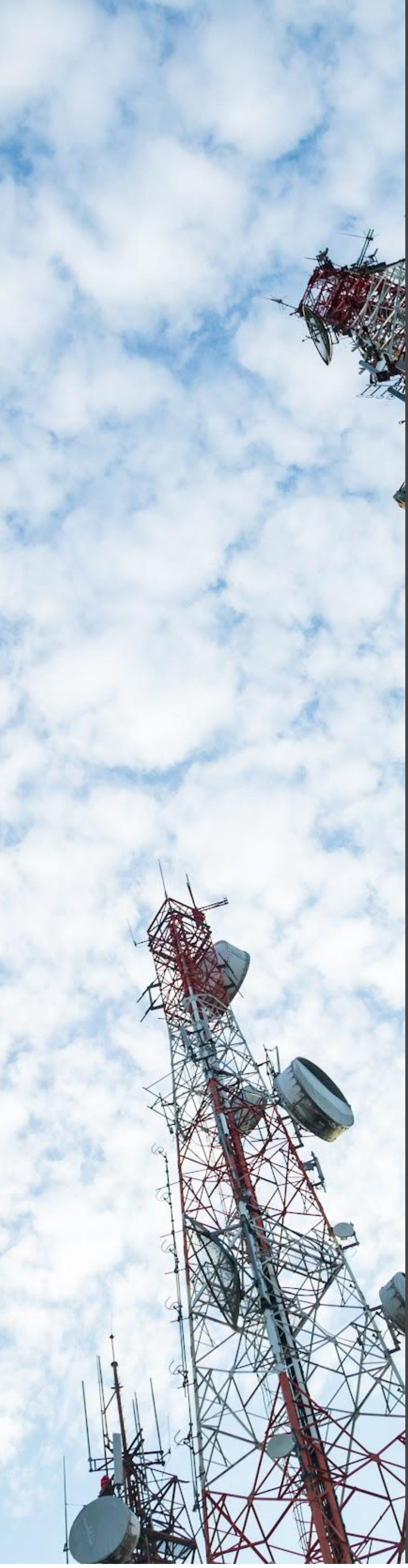
Rajat Chowdhary
Partner, Technology
PwC Middle East
Mobile: +971504293733
Email: rajat.c.chowdhary@pwc.com

Public safety is at the heart of any leading global city’s aspiration. Public Safety Agencies (PSAs) are tasked with the responsibility for protecting residents and visitors. This means implementing cutting-edge safety systems and processes which not only tackle crime and keep citizens safe, but also enable a fast response to emergency situations. One key aspect of such a safety ecosystem is the communication infrastructure, in the form of mission-critical communication systems.

Traditionally PSAs in the field have used individual push-to-talk radios to communicate among themselves and with their respective dispatchers often resulting in siloed communication.

To overcome the limitations, mission-critical communication systems are moving towards adopting open standards in order to leverage emerging technology 5G, immersive applications, real time video, Ultra Reliable Low Latency Communication (URLLC), Isolated Operations for Public Safety (IOPS), advanced congestion management, critical machine type communication, Device to Device (D2D) using sidelink and others which allows enhanced situational awareness and mission-critical grade Quality of Service (QoS) – priority, pre-emption, availability, security, and resilience – that first responders demand.

This paper outlines what it will take for nations to adopt the next generation mission-critical communication systems.



Peter Clemons
Founder & President
Quixoticity-EU
Mobile: +33674123254
Email: peter@quixoticity.com

Having written my first TETRA report back in 1996, and having served as Director and Board Member of the prestigious TETRA Association (now TCCA), I am well aware of the enormous contribution TETRA has made, and continues to make, to global emergency response, and the countless lives it has saved over the past two decades or so.

As we emerge from the global pandemic to a new world with fresh challenges, we need to build on past successes by completing the move to the next generation of mission-critical communication systems based on 3GPP standards LTE/5G, which will allow users to access a wide range of future-proof advanced services and applications requiring high-speed data, big data and analytics and real-time video. Crossing the chasm from narrowband to broadband is the greatest challenge facing our community. This White Paper describes the key stakeholders, drivers and bottlenecks, as well as setting out a roadmap for success.

PwC and Quixoticity-EU look forward to engaging with the wider community and all relevant stakeholders over the coming months and years to agree on the ideas, insights and actions required to successfully complete this journey.

Introduction

Over the past decade or so, the global public safety community and its allies – what we call the Mission-Critical Communications Ecosystem (MCC-ECO) in this paper – have made great strides towards unified next-generation mission-critical communication systems based on broadband technology, these will serve first responders and other critical users for the next decade and beyond.

However, many agencies have faced significant challenges and often considerable delays during their migration from existing, legacy, tried, tested and trusted narrowband to emerging, next-generation broadband solutions. This has created a chasm that can only be crossed with the concerted efforts of the entire MCC-ECO described in the next section. Countries including South Korea, the United States, Finland and the United Kingdom are leading by example in showing the way and providing valuable experiences to a growing number of followers. Going forward, we expect these pioneer countries to continue re-defining the precise nature of the chasm.

This white paper sets out the strategy, drivers and framework for identifying and visualising the critical path for next-generation MCC-ECO acting as a call to action for the ecosystem to take the bold steps required to cross the chasm and enter a new era with confidence, boldness and determination.

Scan to view
the introduction

MCC-ECO - Who are the different stakeholders?

Today, emergency incidents are rapidly evolving and in order to effectively tackle them, there is a need for a comprehensive MCC-ECO. A number of stakeholders must come together to create a robust MCC-ECO. (Figure 1)

A robust MCC-ECO is expected to optimise investments, provide user-centric solutions, and drive interaction models. This ecosystem will comprise multiple commercial, industrial and government agencies coming together to achieve a country's public safety vision.

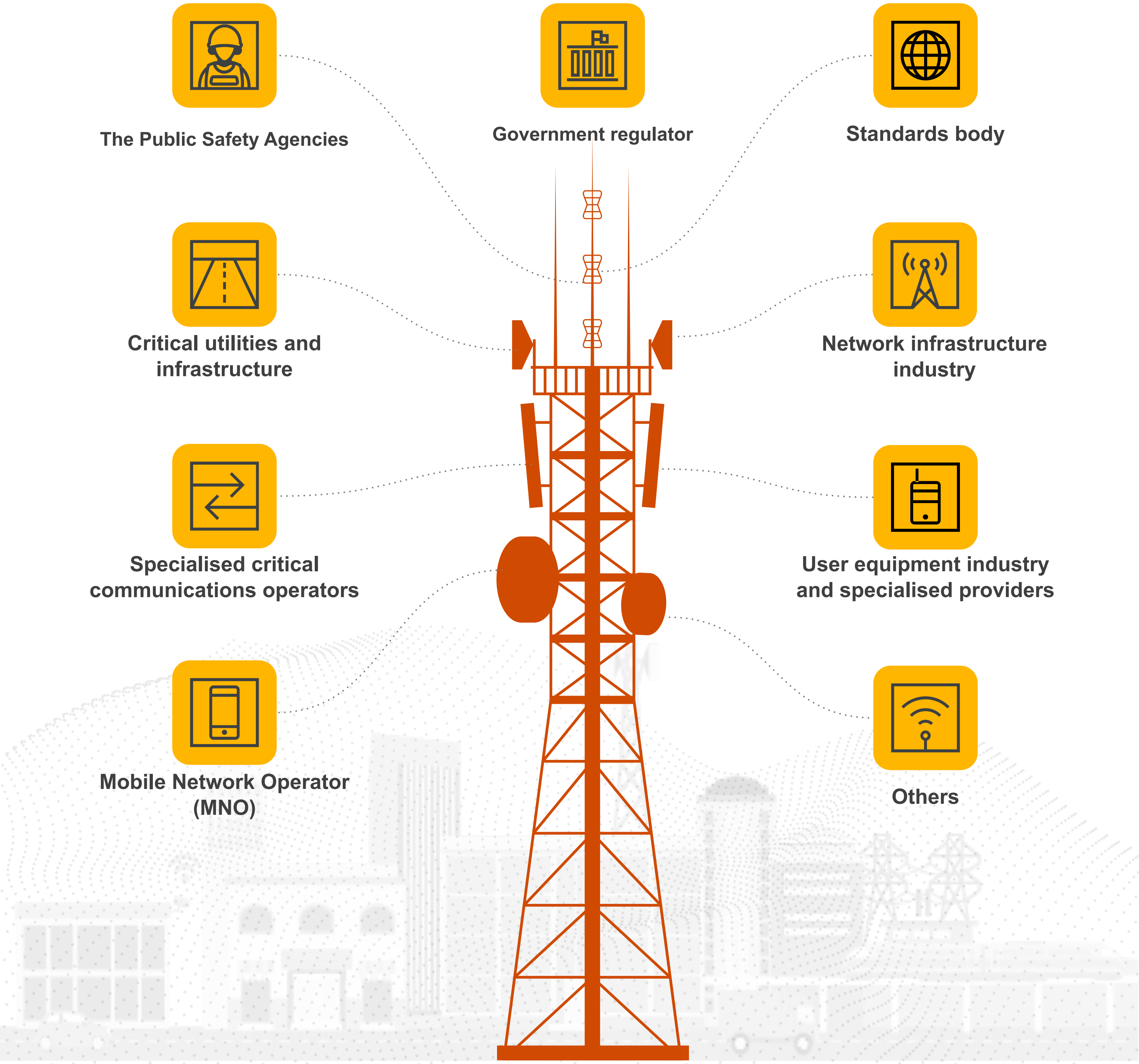

The Public Safety Agencies
Government regulator
Standards body
Critical utilities and infrastructure
Network infrastructure industry
Specialised critical communications operators
User equipment industry and specialised providers
Mobile Network Operator (MNO)
Others

Figure 1: MCC-ECO

Let us take a look at the various stakeholders comprising the MCC-ECO and how they play their respective parts

Government regulator: Responsible for meeting country-wide public safety strategic objectives, providing funding, governing the project, and providing guidance and resources to the programme.

The PSAs: Users of mission-critical communication systems, they are the first responders when emergencies occur and are entrusted with the responsibility of citizens' safety. These include police, defence, health & safety and fire authorities.

Critical utilities and infrastructure: These are vital assets across the country (both private and public) that need a robust mission-critical communication system. This system for assets (such as metros, railway, ships, stadiums etc) usually integrate with the city wide mission-critical communication program.

Specialised critical communications operators: A number of specialised operators - mostly government-owned with exceptions such as the UK's Airwave or Spain's Telefonica - run nationwide public safety networks, and are expected to continue to play an important role in the broadband world. These operators are responsible to governments and end-users, but also have an important relationship with MNOs.

MNO: The MNO is a services provider that owns or controls all the elements necessary to sell and deliver services to an end-user, including radio spectrum allocation, wireless network infrastructure, backhaul infrastructure, billing, customer care, provisioning computer systems, and marketing and repair organisations.

Standards body: Provide the framework and guidelines that the MCC-ECO stakeholders need to conform to when designing, testing and deploying mission-critical communication systems. 3GPP is the globally recognised body for developing the required specifications that are adopted as national and regional standards. Standards bodies that liaise with 3GPP include IETF, IEEE, O-RAN Alliance. There are also a multitude of industry associations such as TCCA, 5G/ACIA, 5G/AA that feed user requirements into these standards bodies.

Network infrastructure industry: Network services provider of the core systems for managing the network and key data systems and ensuring data security and preparedness. This includes radio access networks consisting of hardware, software and services. Its portfolio includes products in the areas of antenna, radio, RAN Compute, site and transport solutions – all managed by a common management system.

User equipment industry and specialised providers: Includes handheld devices that are used by the PSA users to communicate with one another (and preferably interoperable to avoid lock-in to one brand). Specialised providers design the mobile app for the user equipment for first responders and provide services such as real-time video transmission and MCPTX implementation.

Others: The MCC-ECO will also incorporate new players such as global hyper-scalers and more local service providers offering cloud and edge computing services. Critical Internet of Things (IoT) services requiring field devices such as body-worn cameras, heart-rate detectors, man-down sensors, and drones using emerging technologies will encourage even more players into the broadband public safety market.

Building and operating mission-critical communication systems can deliver next-generation connectivity, but for enhanced usability, robust performance and flexibility a comprehensive ecosystem is required.

Ensure optimum participation from all stakeholders to achieve maximum potential.

Enable clear roles and responsibilities for all stakeholders

Adopt emerging technologies and trends across the ecosystem

Global examples

Finland

The Finnish critical communications ecosystem has been named a top performer in the sector. Finland built an ecosystem of solutions and service providers that enables packaging of their solutions and is replicable across countries. Their current system has seamless cooperation between agencies within Finland and the potential and ability to work with networks in other neighboring countries, as well as the EU BroadWay project. (Figure 2)

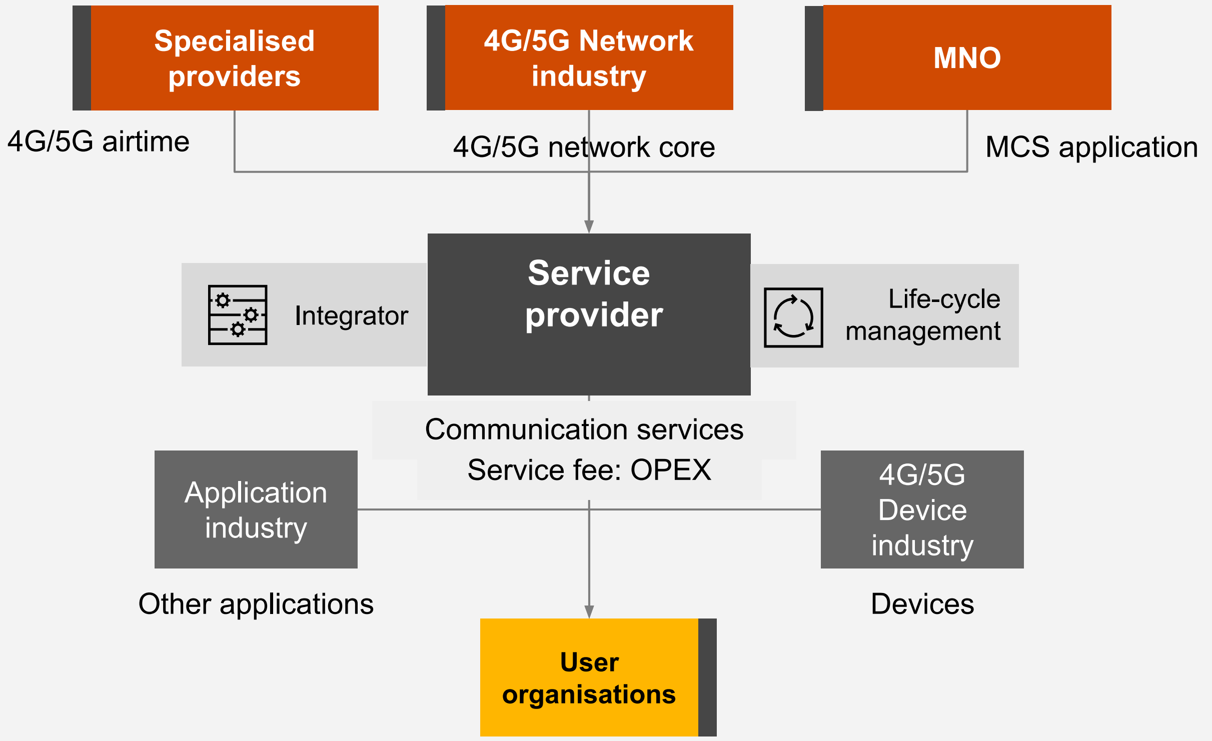
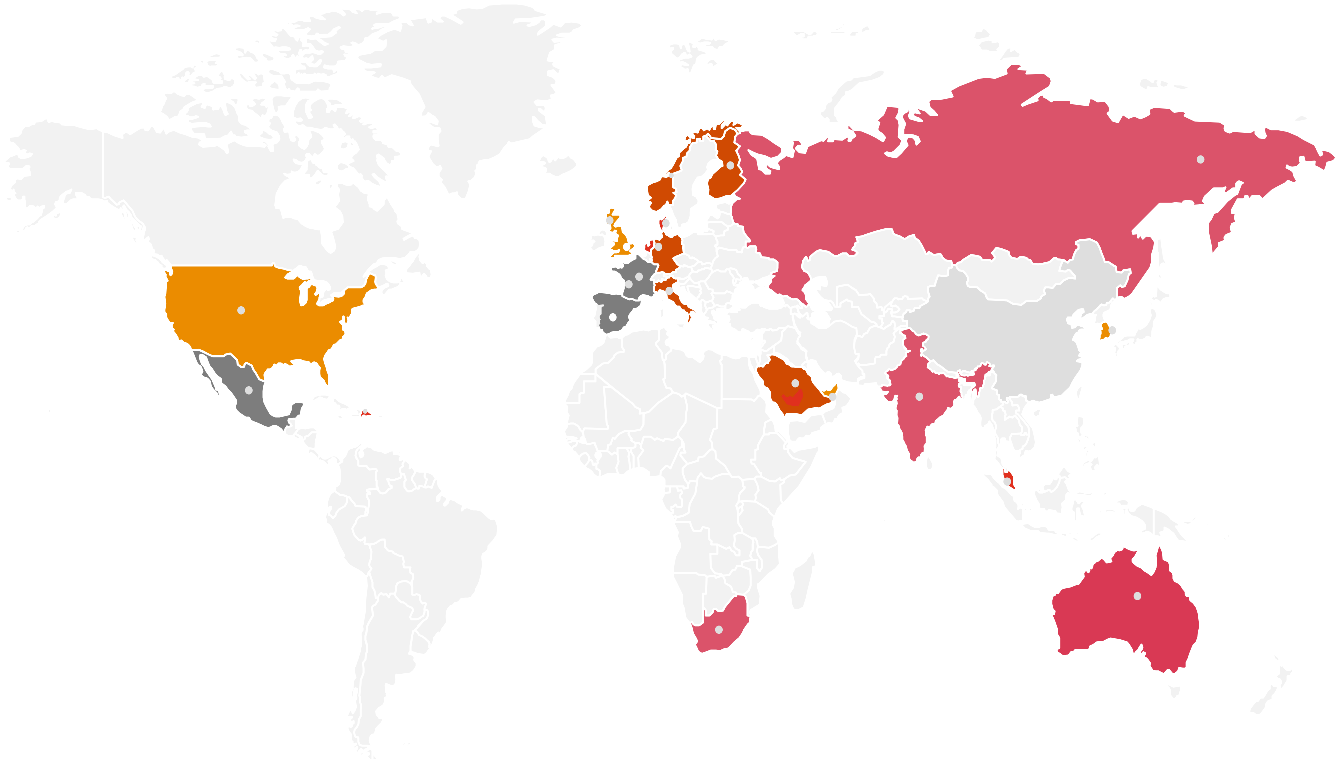


Figure 2: VIRVE 2.0 ecosystem interaction model

Figure 2 displays the Finnish VIRVE 2.0 ecosystem interaction model enabled by the inherent Finnish culture.The model advocates close collaboration between different agencies, complimented by a robust MCC-ECO.This has set an example for other nations to follow.

Global snapshot of mission-critical communication programme deployment

Enhanced, data-rich communications will provide better situational awareness in times of emergencies, and in everyday life. The PSA and government agencies' mission-critical communication market is expected to reach US$9.39 billion by 2028 from US$5.81 billion in 2021; it is estimated to grow at a CAGR of 7.4% from 2021 to 2028 (2).



Nationwide LTE

United Kingdom

- 'Airwave' and 'ESN' Nationwide TETRA+ LTE

United States of America

- 'FirstNet' Nationwide LTE

South Korea

- 'SAFENet' Nationwide LTE

United Arab Emirates

- Dubai (Nedaa): city wide TETRA network + broadband network & Citywide LTE network *(significant dedicated spectrum in 700 MHz)*
- Abu Dhabi: TETRA+ Public LTE+ Private LTE

Nationwide TETRAPOL

Mexico

- Nationwide TETRAPOL (AIRBUS) 200,000 users, 32 states and about 200 municipalities.

Switzerland

- Nationwide TETRAPOL (Polycom)
- Moving to broadband (MSK)

France

- PCSTORM, Nationwide TETRAPOL now moving to LTE (RRF)

Spain

- Country wide Tetrapol system – Sirdee

Nationwide TETRA

Kingdom of Saudi Arabia

- Various PS entities have own TETRA network and there is movement towards nationwide LTE

Belgium

- 'ASTRID', Nationwide TETRA

Germany

- 'BOS' Largest TETRA Network in the world (1 million users)

Singapore

- Nationwide TETRA

Denmark

- Nationwide TETRA

Italy

- Programma Interpolizie TETRA, Nationwide TETRA

Finland

- 'VIRVE' Nationwide TETRA moving to VIRVE2.0 (LTE)

Norway

- Country wide TETRA- Nodnett

Dominican Republic

- Country wide TETRA with 20 base stations and Hytera system

Siloed mix

Russia

- Siloed Analog + TETRA + LTE

India

- Siloed Analog + TETRA

Australia

- Statewide P25 and now moving to LTE (Public Safety Broadband Network)

South Africa

- Siloed Analog + TETRA

Figure 3: World map of MCC deployment

The majority of governments continue to invest in traditional technologies while starting to engage with MCC-ECO stakeholders to move towards broadband communications systems; few countries have leapfrogged to nationwide mission-critical communication over 4G/LTE. **(Figure 3):**

Each country has embarked on its mission-critical communication journey shaped by various drivers **(Figure 4)** such as the potential impact from external factors (including accidents, emergencies and potential threats), funding strategy, governance structures, vendor lock-ins and spectrum bandwidth availability. Although all countries start the journey towards and across the chasm from different positions and with different allocations of resources, there is much to be learned from adopting those best practices from the pioneer nations.

Mission-critical communication programme drivers

Key drivers and examples

Public safety regulations

Ex. Finland has mandated commercial MNOs to give priority to PSA users during emergencies

Public safety governing agency

Ex. A dedicated agency governing the network Safe-Net Forum - South Korea

User and stakeholder requirements

Ex. PSA users in UK pushed for key functionalities to be made available in ESN before going live

OEM presence and partnerships

Ex. Samsung has partnered with South Korea Safenet to deliver 3GPP-compliant country-wide LTE MCC system

Spectrum allocation

Ex. USA has dedicated band 14 for PSA users

Mandates, priorities & existing initiatives

Ex. UK to build a secure and resilient mission-critical communications network the emergency services can trust to keep them safe

Crisis and emergency events

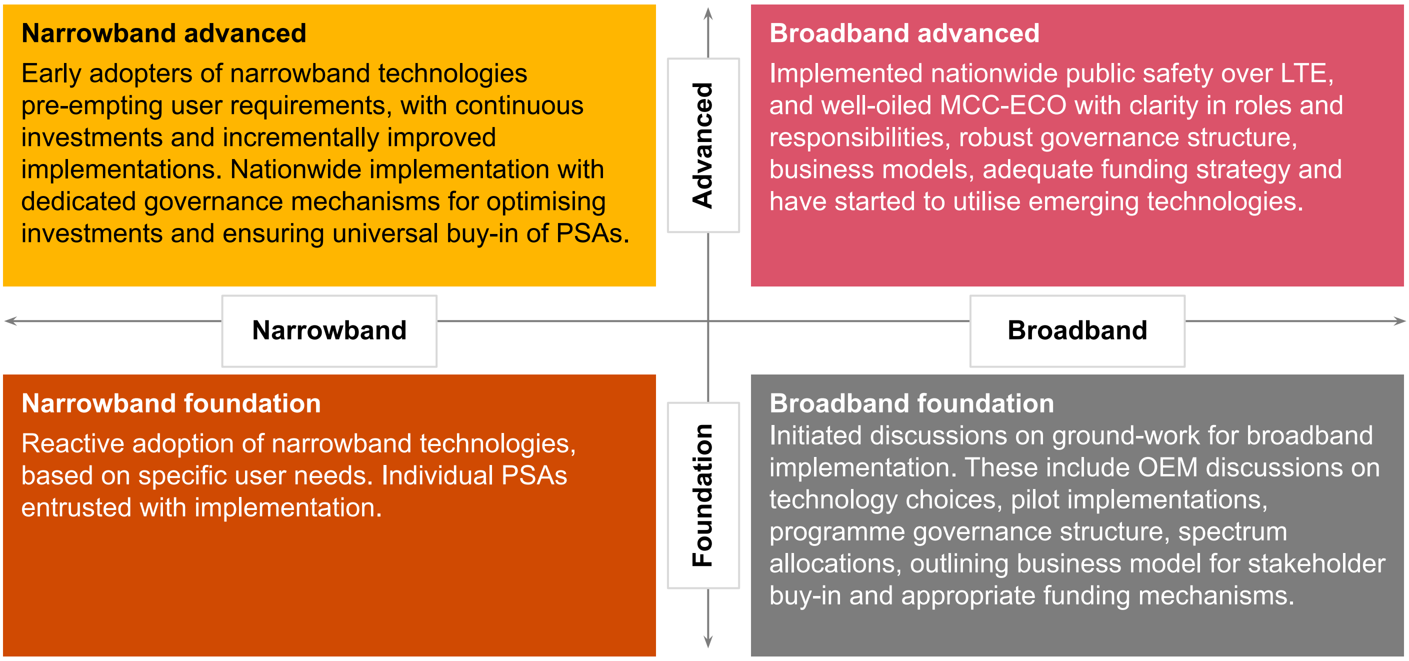
Ex. Triggered by a catastrophic emergency event in the US

Existing technology investments

Ex. US is investing $46m towards network enhancements

Figure 4: Key mission-critical communication programme drivers

Real world implementations of a MCC-ECO based on broadband show that countries fall into four main categories **(Figure 5):**



Narrowband advanced

Early adopters of narrowband technologies pre-empting user requirements, with continuous investments and incrementally improved implementations. Nationwide implementation with dedicated governance mechanisms for optimising investments and ensuring universal buy-in of PSAs.

Broadband advanced

Implemented nationwide public safety over LTE, and well-oiled MCC-ECO with clarity in roles and responsibilities, robust governance structure, business models, adequate funding strategy and have started to utilise emerging technologies.

Narrowband foundation

Reactive adoption of narrowband technologies, based on specific user needs. Individual PSAs entrusted with implementation.

Broadband foundation

Initiated discussions on ground-work for broadband implementation. These include OEM discussions on technology choices, pilot implementations, programme governance structure, spectrum allocations, outlining business model for stakeholder buy-in and appropriate funding mechanisms.

Figure 5: Mission- critical communication technology vs. maturity categories

The evolution of PSA communication systems towards hybrid and eventually pure-play mobile broadband systems is a fundamental shift of the MCC-ECO. Existing transformation programmes can be mapped to provide an overview of this evolution as individual countries move towards their desired end-states. **(Figure 6):**

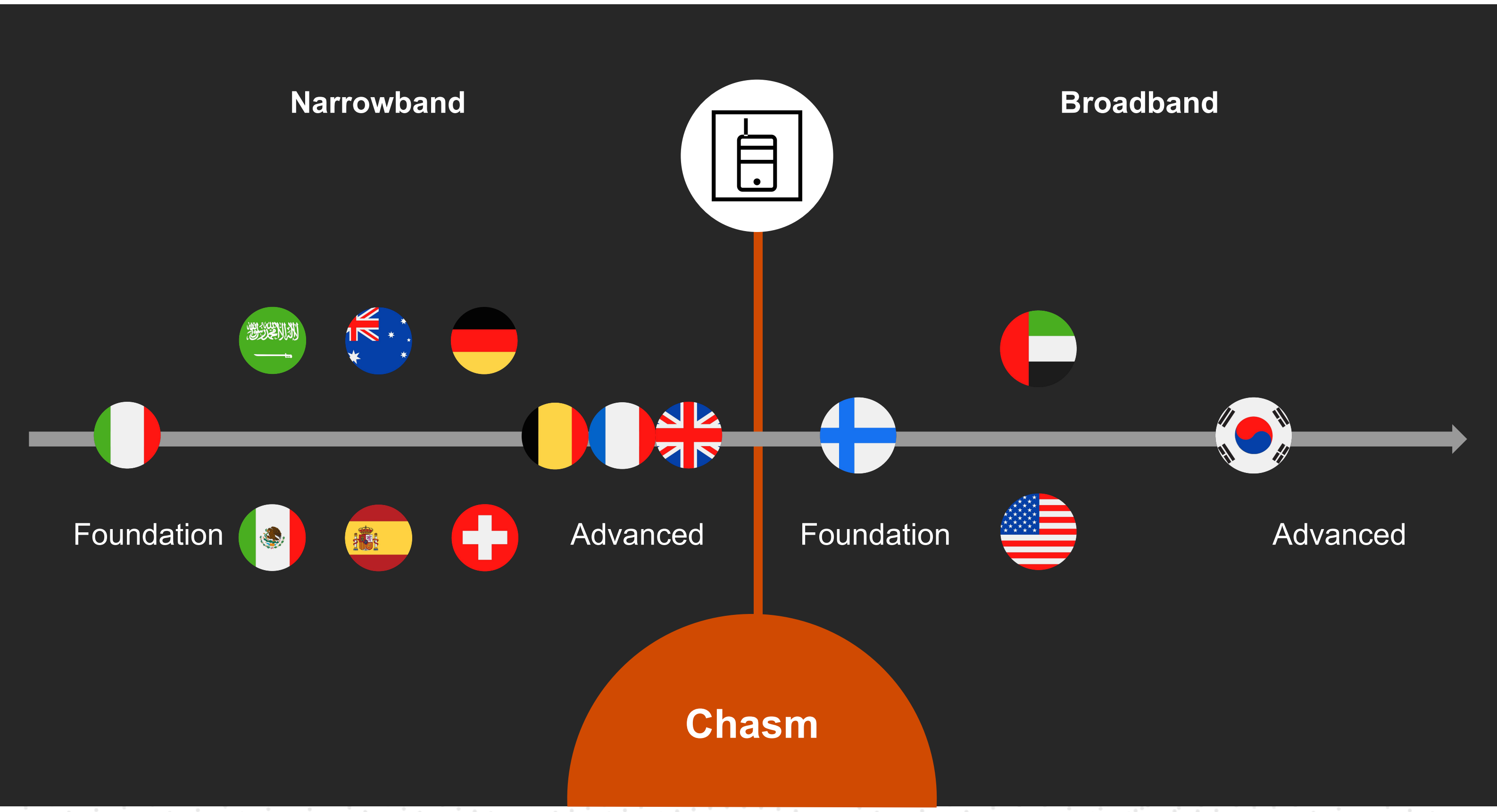


Figure 6: Mapping of countries' mission-critical communications programmes

Please refer page 20 for understanding our point of view on positioning these countries

Global examples

South Korea

Korea's Safe-net is the World's first 3GPP-compliant nationwide Public Safety LTE (PS-LTE) network, aspiring to move to 5G as soon as the standards are defined. The nationwide Safe-net programme is centrally governed by the Ministry of Interior and Safety, clearly outlining stakeholder roles and responsibilities.

It is the first 3GPP-compliant PS over LTE implementation, and cooperates with The Critical Communications Association (TCCA) to provide standards, guidelines and policies for the Safe-net Forum.

The programme is sponsored by the Ministry of Interior and Safety, and the setup cost is shared with a commercial MNO. It utilises a dedicated spectrum allocation of 700 MHz band 28 for seamless communication and operations.

The programme has a dedicated core operated by Safe-net interconnected to the RAN of several operators, thus avoiding any potential OEM lock-ins.

The end-state of South Korea's Safe-net network will produce a public safety service that:

Provides secure mission-critical mobile broadband compliant with the latest 3GPP standards releases.

Ensures wide geographic coverage with enhanced quality of service.

Utilises numerous emerging technologies such as IoT, AI, big data, drones, robotics, wearable devices, and others.

What does the end goal look like?

The MCC-ECO stakeholders understand the urgency of moving to a full broadband solution. There are a growing number of pioneer and early follower countries that have made significant progress towards full mobile broadband solutions based on LTE, with a future path to 5G as the standards are completed. Much of the legislation, regulation, standardisation, and technical and organisational developments are in order to drive forward country-wide processes.

The following non-exhaustive list of key features of a future broadband-based mission-critical communication systems' capability gives a clearer idea of what the target state looks like. By providing all of these features, the MCC-ECO will be capable of crossing the chasm and opening up new possibilities for mission-critical services in today's broadband/5G era.

360° control and security

There is a growing consensus within the global public safety community that a dedicated public safety core network is required, with the final goal being a 5G stand-alone core, including 5G NR voice services.

Superior quality of service

To achieve all the relevant MCX KPIs, a significant amount of spectrum will be required in low- and mid-bands, working seamlessly with MNO spectrum for extra capacity, which means that a more open approach, such as OpenRAN will be the final goal towards the end of this decade.

Anytime, anywhere, always connected

Mission-critical systems require extended coverage, with additional sites for remote, rural areas, satellite integration, deep indoor coverage, and national and international roaming.

End-to-end futureproof service portfolio

The final goal is fully standardised MCPTX (voice, data video, multimedia/XR) services, including control rooms, dispatch and inter-working functions (IWFs).

Enhanced situational awareness

Real-time on-the-ground information enabled by control room integration with full AI/ML-driven data analytics and predictive capabilities.

Moving to a full broadband mission-critical communications system is not just about replacing existing procedures and services. The ultimate goal must be for PSAs to move ahead of the commercial curve by adopting more advanced features and devices such as drones, robotics, and real time video streaming. Emergency response can be radically transformed over the next five years by adopting emerging 5G functionality including extended reality, artificial intelligence and fully automated repetitive procedures.

Global examples

United States of America

FirstNet was built with a vision to create a dedicated and differentiated broadband communications experience that transforms public safety operations to save lives.

Number of users **3.3 M+**

20,500+ agencies on FirstNet

190+ apps in the catalogue

Square miles of coverage **2.81M+**

Number of connections **3M+**

FirstNet ready devices **370+**

It is vital to stay connected and be able to communicate in critical circumstances. For example, in 2021, Oregon's Bootleg Fire turned into the nation's largest active blaze, destroying more than 400 buildings and hundreds of vehicles. To combat this emergency, **more than 1,000** first responders across multiple agencies were deployed. At the time, FirstNet deployed dedicated portable network assets (SatCOLTs) to provide fire fighters and other crew members with the dedicated connectivity and 'always on' priority communications they require, facilitating a higher level of safety on the ground by providing better situational awareness via applications, near real time footage and communications.

How to cross the chasm and unlock the full value of next generation critical communications?

To cross the chasm and reach the desired end state of full 5G functionality, authorities and PSAs, working closely with the full MCC-ECO, will collectively need to overcome a number of bottlenecks still currently holding them back. Individual agencies, and even nations can no longer make decisions in isolation without studying and understanding global trends; traditionally conservative organisations need to be more open to challenging long-held beliefs and changing age-old procedures and practices; and finally, closed, proprietary solutions need to be rejected in favour of open, flexible, future-proof solutions that can evolve with the times. In recent years, a growing number of regional and global initiatives have been created that allow the MCC-ECO to overcome the bottlenecks mentioned below.

Siloed mission-critical communication programmes

Global cooperation amongst countries is imperative for their mission-critical communications programmes to take appropriate learnings and preempting failures. This can also impact conforming to standards, spectrum allocations, rolling out legislation and regulation to create a common, predictable environment for key stakeholders to fund initiatives.

Lack of change management

People within organisations become used to working in a particular way, so change can be very challenging. Training and also convincing users that new solutions are as safe and secure as the ones being replaced, is critical. A clear vision and strong, decisive leadership at multiple levels is key here.

Vendor-locked solutions

The proprietary, black-box approach from vendors is no longer acceptable in today's world. In fact, it has been shown that open source solutions can actually be more secure, although supply chains must be vetted carefully by national PSAs. Systems needs to be secure by design and open to scrutiny based on global standards supported by a competitive, multi-vendor ecosystem.

There are a series of stages that all authorities and agencies will need to pass through to cross the chasm from narrowband to broadband and reach the target state. Everything begins and ends with satisfying user requirements, putting into place all the essential building blocks such as standards, spectrum and the right mix of products and services.

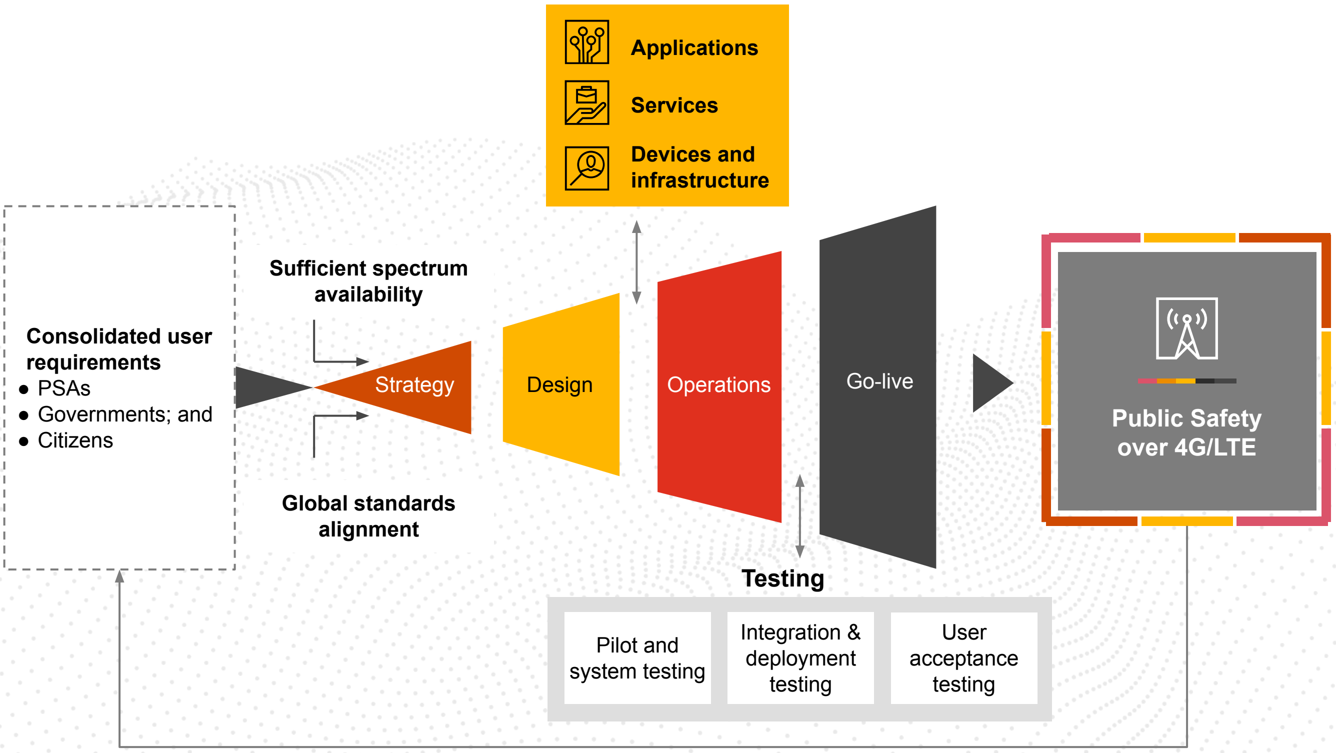
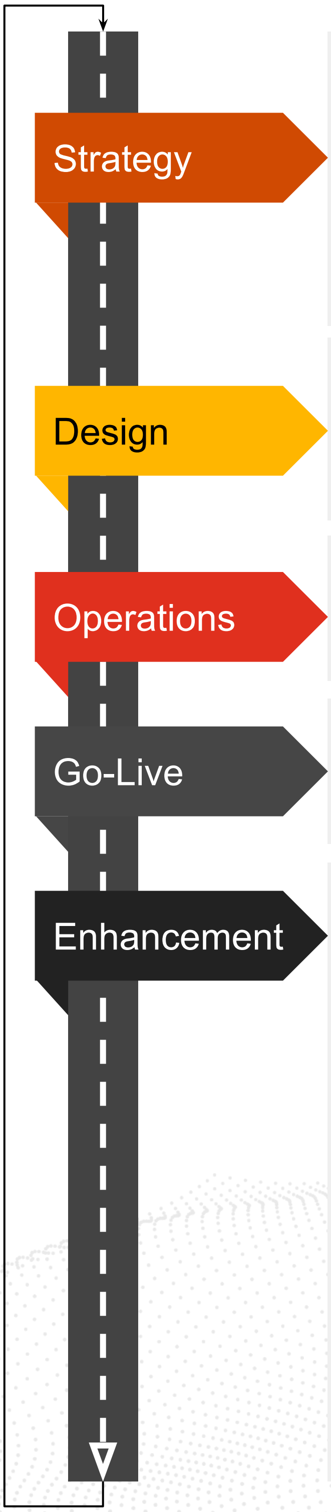

Applications
Services
Devices and infrastructure
Consolidated user requirements
● PSAs
● Governments; and
● Citizens
Sufficient spectrum availability
Strategy
Global standards alignment
Design
Operations
Go-live
Public Safety over 4G/LTE
Testing
Pilot and system testing
Integration & deployment testing
User acceptance testing

Figure 7: Framework to cross the chasm

There can be various initiatives at each stage of the framework. Each individual initiative below is important in its own right, but when we bring all of these together and when the MCC-ECO collaborates for the common good and is focused on achieving the desired end-state set out in this paper, then ultimate success is practically guaranteed.



United States NIST **Public Safety Communications Research Division** (PSCR) was set up in 2002 following 9/11 and in 2012 was assigned US$300 million following the setting up of FirstNet to fund primary research into innovative public safety solutions. **European Commission** has provided funding for the 3-phase, pre-commercial procurement, **BroadWay** programme set up in 2017 and now in its final pilot phase with consortia led by Airbus DS and Frequentis, which is developing and enabling a pan-European public safety mobile broadband system.

3GPP works on global standards for mobile cellular communications and has been the home for mission-critical services (MCPTT/Data/Video, i.e. MCX or MCPTX) standardisation since SA Working Group 6 was set up in late 2014, encouraging a growing MCC-ECO collaborating within the standards process.

ETSI has been carrying out MCPTT/MCX Plugtests since 2017, bringing together the global MCC-ECO to validate the 3GPP standards work as well as the interoperability of a wide range of MCX/FRMCS products and services.

Building upon its successful TETRA Interoperability Profiles (TIP), **TCCA** has partnered with **GCF** to start building a testing and certification regime for mission-critical solutions based on 3GPP technologies.

Following a meeting of early pioneers in public safety broadband initiated by US FirstNet in 2016, during a meeting of 80 representatives from 19 countries in Boulder, Colorado in 2019, it was agreed to set up the annual **Global Public Safety Operators Conference (GPSOC)** to allow agencies to exchange ideas and experiences, although COVID has prevented the conference actually taking place since then.

Critical communications world is the premier global annual event organised by TCCA that brings together thousands of people from the MCC-ECO and related sectors to discuss the current status and evolution of the industry. It evolved from the TETRA World Congress, that began in 1998, and the most recent edition is being held in Vienna, Austria from June 21-23, 2022.

Quixoticity Index is a report launched in 2017, starting with 10 countries, intending to provide a framework for understanding current and future trends within critical communications within a 2030 horizon incorporating the United Nations Sustainable Development Goals (SDGs). A new, fully updated edition is planned for early 2023.

It is also important to reiterate that once the full solution has been developed,it should be refreshed and updated periodically, which should be much easier to achieve due to the new, more open way of working and software based approach.

Some of the pioneer nations mentioned in this paper have required as long as a decade to move from the initial concept to final state, and some of these still have to undertake the final part of their journey. It is therefore vital for the perceived laggards not to wait until the full solution has been adopted by others, as valuable lessons can be learned by actually treading the path oneself and moving forward from one stage to the next.

How can we help you achieve your goals?

We are strongly committed to providing governments as well as critical infrastructure entities with the tools required to develop or continue progressing their MCC-ECO. PwC can provide support throughout the mission-critical communication programme (MCCP) journey; from creating the initial strategy, to building the infrastructure (technology selection and MCCP concept of operations), to assisting in the development of your operations in terms of operating model, RFP and vendor evaluation, to the final step of ensuring a smooth launch of the mission-critical communications system.

Strategy	Design		Operations		Go live
1	2	3	4	5	
MCCP user requirements and business case	**MCCP technology selection and command centre**	**MCCP CONOPS**	**MCCP operating model**	**RFP and vendor evaluation**	**Project management and testing**
• Assessment of the existing MCCP • Perform risk assessment to identify the risks/threats that MCCP will handle • Benchmarking study for alignment and best practices • Defining MCCP objectives • Developing use cases/ capability of the MCCP • MCCP strategic context including business case and return over investment	• Network components design and location assessment • Communication technology selection (TETRA, P25, LTE, 4G/5G, Hybrid etc) • Design of MCCP Command Control Center (CCC) including ISO 11064 compliance (airflow, lighting, acoustics, ergonomics etc) • 2D/3D architectural layout (elevation) • Design of integrated building management system • CCC IT infrastructure and network design	• Mission-critical communications platform design tenets • Detailed platform architecture including integration requirements • Identify list of key OEMs for the mission-critical communications platform • Defining CONOPS and SOP • Simulation of use cases on digital twin/emerging technology • MCCP user journey maps highlighting interaction points (external and internal stakeholders)	• Define department vision and mandate • Align with enterprise crisis management and BCM Framework • Organisational structure and people requirements • Define governance structure (incl. KPIs, decision rights, RACI Matrices) • Develop business continuity plan for MCCP department • Perform technology impact analysis and identify recovery objectives for the IT applications/services used by MCCP	• RFP preparation including pre qualification, technical evaluation, scope of work, technical/ functional specifications • Define service level agreement parameters for different components • Support on pre bid meeting and clarification response • Vendor response analysis (technical and commercial)	• Project management activities including risk mitigation and daily project coordination to meet project milestones • Supply installation testing (use case testing) & go-live monitoring • SLA monitoring for the edge devices, applications and IT infrastructure • Evaluation of the change requests across project lifecycle

MCCP development stages

Conclusion

Great progress has been made over the past decade or so by the global public safety community to develop truly global standards for mission-critical communication systems together with other key industry players

Enormous challenges are facing us during these unprecedented times presenting truly existential threats that need to be addressed promptly and decisively

Time is not on our side so we must move faster to remove the remaining bottlenecks to full adoption of next generation mission-critical solutions and unlock their full social value. This will require a collective effort of the whole ecosystem working together

The journey continues. PwC and Quixoticity-EU will be there every step of the way to help the MCC-ECO cross the chasm and reach the promised land of sustainable, future-proof, full 5G-enabled mission-critical services that will enable the better, smarter, safer world of 2030.

References

1. https://www.3gpp.org/about-3gpp/about-3gpp
2. https://ec.europa.eu/eurostat/cros/content/Glossary:Mobile_network_operator_(MNO)
3. https://tcca.info/about-tcca/
4. https://www.cbsnews.com/news/bootleg-fire-oregon-update/#:~:text=A%20wildfire%20raging%20in%20Oregon,homes%20under%20mandatory%20evacuation%20orders.
5. https://blogg.telia.se/app/uploads/sites/4/2020/03/Bl%C3%A5ljusn%C3%A4t-Finland.pdf
6. https://www.keytouch.online/stories/the-worlds-safest-rally-relies-on-virve
7. https://www.capgemini.com/wp-content/uploads/2021/01/Whitepaper-Mission-critical-communications-for-Public-Safety.pdf
8. https://www.erillisverkot.fi/en/virve-rakel-and-nodnett-successfully-together/
9. https://www.nodnett.no/english/information-in-english/international-collaboration/

Annex

Australia	Having previously struggled to move forward with its nationwide public safety broadband network plans, NSW Telco Authority has taken a lead in procuring a Proof of Concept (PoC) public safety LTE capability from Nokia with MNO partners, Optus and TPG Telecom
Belgium	Specialised operator, ASTRID, has been operating a mobile broadband service, Blue Light Mobile, as MVNO for several years now, although this service is not regarded as mission-critical.
Finland	Erillisverkot has awarded contracts for a dedicated core to Ericsson and radio access network to MNO, Elisa, and plans to start data services during 2022.
France	The tender for the ambitious RRF (Future Radio Network in English) programme is currently ongoing, with plans to set up a new specialised operator, ACMOSS to run the nationwide public safety network that needs to be up and running in time for the 2024 Paris Olympics.
Germany	BDBOS plans to continue running TETRA into the next decade. However, it has recently conducted trials with 2 German MNOs to test certain mission-critical broadband features and is actively searching for sufficient dedicated spectrum in 470-694 MHz.
Italy	Italy has struggled to build a full nationwide TETRA capability comparable to other European nations, falling back on other analogue and digital narrowband solutions in particular areas and for particular user groups. A public safety broadband PoC has been carried out with Telecom Italia.
Mexico	The country has a mix of a federal TETRAPOL network and state-wide TETRA networks for public safety and government services. It was decided to build a shared network, Red Compartida run by Altan Redes, in 700 MHz which can also be used for public safety broadband services under MVNO model.
Saudi Arabia	There is a patchwork of multiple TETRA - and LTE - networks run by ministries across the Kingdom, with very limited interoperability. Dedicated spectrum has been awarded to public safety in 800 MHz, but as yet, no network has been rolled out in this band.
South Korea	Following a tragic ferry accident in 2014 where hundreds of people, including school-children, lost their lives due to a lack of communication among first responders, the Korean Government became more active within 3GPP public safety broadband standardisation and set up SafeNet Forum. Multiple dedicated LTE networks have been rolled out in 700 MHz band for public safety, railways and maritime users. South Korea is recognised as leading the way globally in this field.
Spain	Back in the late 1990s, the Spanish central government chose Telefonica to run its nationwide public safety network using TETRAPOL technology to allow easier border communications with France during the era of Basque terrorist group, ETA. Most autonomous regions actually chose TETRA for their regional networks. LTE trials have been conducted in 450 MHz and the latest Telefonica contract contemplates the incorporation of a broadband capability during the next 3 years.
Switzerland	Similar to Germany, Switzerland has a decentralised approach to government and public services, with its cantons making the major decisions. Currently depending on a nationwide TETRAPOL network, Switzerland is currently developing its MSK secure broadband programme with pilots being tested in multiple cantons.
United Arab Emirates	Dubai's specialised operator, Nedaa, has rolled out a mission-critical LTE network across Dubai, including for the recent World Expo, with dedicated spectrum in 700 MHz and 2.3 GHz. As well as providing service for public safety agencies, Nedaa also serves industrial and enterprise customers such as Dubai Metro.
United Kingdom	UK Home Office was one of the first government departments back in 2011 to announce plans to build a nationwide public safety LTE network - ESN - to replace the existing TETRA network operated by Airwave. Having awarded contracts back in 2015, multiple delays mean that ESN will not now be fully operational until at least 2024, with the Airwave TETRA network continuing to operate until at least 2026.
United States of America	We have already described the creation of FirstNet earlier in this white paper. FirstNet is currently focused on providing mission-critical data, as there are no plans to close down existing statewide P25 networks yet, although FirstNet has implemented 2 MCPTT solutions that offer similar capabilities.

Contact us

Rajat Chowdhary

Partner, Technology
PwC Middle East
Email: rajat.c.chowdhary@pwc.com

Sharang Gupta

Director, Technology
PwC Middle East
Email: sharang.g.gupta@pwc.com

Vishesh Kalia

Senior Manager, Technology
PwC Middle East
Email: vishesh.k.kalia@pwc.com

Peter Clemons

Founder & President
Quixoticity-EU
Email:peter@quixoticity.com

Contributor

Naela Afifi

Consultant
PwC Middle East
Email: naela.afifi@pwc.com

www.pwc.com/me

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 155 countries with over 327,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 7,000 people. (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.