Advancing Public Safety Critical Communications

The strategic shift to 5G private networks

RESEARCHED BY

OMDIA

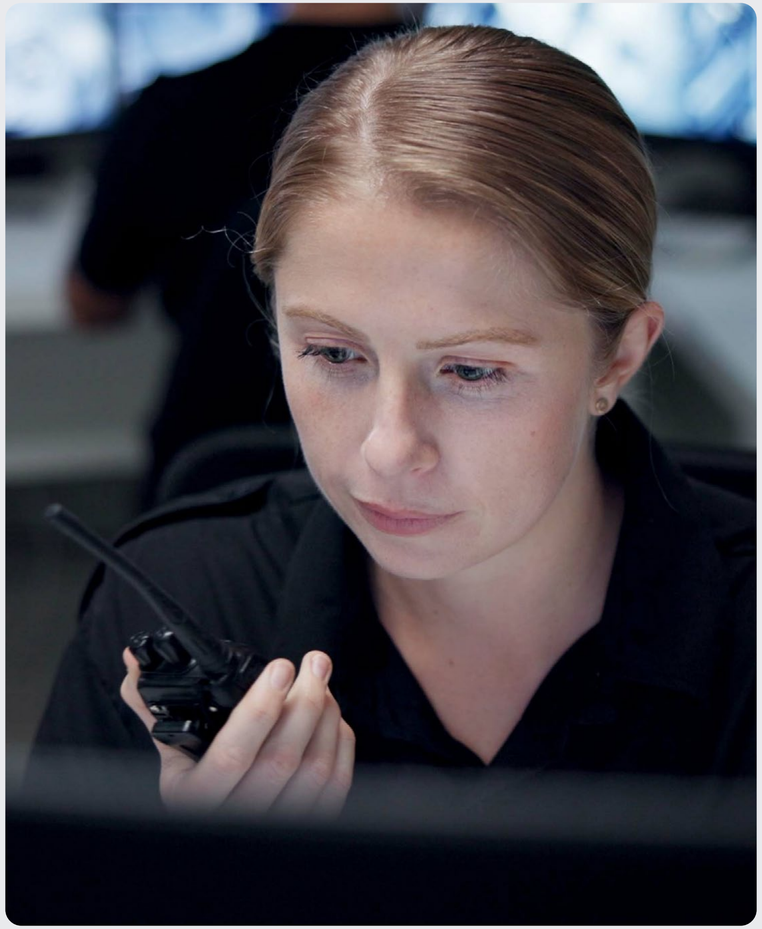
COMMISSIONED BY

NOKIA

CONTENTS

KEY TAKEAWAYS

- Reliable communications have always been the backbone of public safety operations, where lives depend on the speed, clarity, and reliability of every message. Whether coordinating first responders or maintaining real-time situational awareness, effective communication is paramount for those on the front lines.
- For decades, narrowband voice-only private mobile radio (PMR) systems such as TETRA and P25 have served as the trusted standard. But as public safety challenges grow more complex, agencies face limitations in voice-only communication. These legacy systems cannot fully support the real-time data, video, and advanced applications now essential for modern emergency response.
- The adoption of 4G and 5G broadband enables public safety agencies to exchange data-rich content, improving situational awareness and empowering responders with tools such as live video feeds, drone surveillance, and advanced analytics in real time.
- Dedicated broadband networks provide public safety agencies with exclusive resources, secure bandwidth that is both reliable and resilient. Private networks ensure that critical communications remain uninterrupted and secure, even under extreme conditions, and give agencies complete control over their communications infrastructure, enhancing security and compliance. By owning their networks, public safety organizations can maintain the highest standards of data privacy, security, and trust, providing peace of mind in life-threatening situations.
- Private cellular networks that leverage state-of-the-art 4G and 5G technology offer public safety agencies scalability and adaptability, supporting emerging multimedia communications and innovative collaborative applications. This ensures that public safety communications are ready for today's threats and able to adapt and face the challenges of tomorrow.



RECOMMENDATIONS: FOR PUBLIC SAFETY AGENCIES AND GOVERNMENTS

1. **Take proactive steps toward adopting dedicated private 4G and 5G networks to future-proof communications infrastructure**. Broadband adoption enables public safety agencies to build resilience into their operations and set a strong foundation for handling increasingly complex emergency scenarios.
2. **Establish a dedicated network core and allocate resources to make sure communications are always reliable and secure.** By retaining exclusive control over the core network, public safety agencies can guarantee high-priority bandwidth, minimize downtime, and maintain robust security for mission-critical communications..
3. **Plan for future growth and technological advances by selecting solutions that offer modularity, upgradability, and scalability.** With a flexible network design, public safety agencies can easily upgrade their networks and integrate new capabilities such as video, Internet of Things (IoT), and advanced analytics, ensuring the system remains reliable and effective for years to come.

An introduction to public safety critical communications

In recent years, the world has witnessed a surge in emergency incidents, both natural and human-made, posing unprecedented challenges to public safety. From devastating earthquakes to acts of terrorism or civil disorder, the increasing severity and complexity of these events underscore the critical role of emergency responders in safeguarding communities and saving lives.

At the heart of effective emergency response lies a robust communication system. For public safety professionals, the stakes are extraordinarily high: they routinely put their lives on the line to save others and deal with critical threats. A resilient network is essential to serve as a lifeline during their missions, ensuring real-time communication between field agents and dispatch centers even in the most challenging circumstances. These communications systems enable public safety agencies to coordinate rapid responses, exchange vital information, and make informed decisions under pressure. For public safety users, communication systems must meet exceptionally high standards in terms of reliability, effectiveness, and security.

As the backbone of emergency operations, these critical communication systems empower responders to minimize response times, gather and share detailed situational data, and plan and execute strategic interventions.

In essence, mission-critical services (MCX) communication technology are not just tools but vital assets that have a direct impact on the success of emergency responses, the safety of communities, and the preservation of human lives in times of crisis.

Mission-critical communications

Capture

Exhaustive data collection

Several mechanisms that enable data collection (CCTV, sensors, body-worn cameras)

See

Efficient visualization tools

Analysis of the data and presentation to the command room and agents in the field

Manage

Communication technology

Mission-critical communication technology connecting individuals and groups

Remember

Archiving and storage

Databases of policing data and all the relevant information

Predict

Analysis of information

Artificial intelligence / big data

SOURCE: OMDIA

Trends shaping the public safety communications market

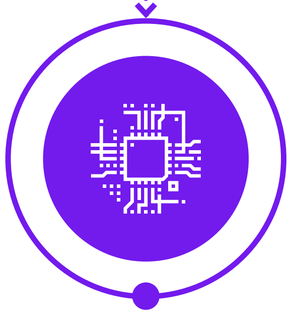
MCX technology is no stranger to transformation, but in this industry, a calculated and trustworthy evolution is key for reliable support of complex emergency responses. To guarantee services under any circumstances, critical communication systems must be rock solid. Overtime, it must adapt and overcome the evolving threats that could compromise the operations of public safety agencies.

The perfect example of this evolution is the digitalization transformation from the legacy analog systems used by the public safety communications vertical. Digital radios not only provide longer battery life, better sound quality, and stronger inherent signal security than analog but also offer spectrum efficiencies and a strong flexible platform that users can adapt to meet their needs.

When confronted with major shifts in technology, disruptive transformation is not an option for governments and public safety stakeholders, because the reliability of the network and the services must always be prioritized.

MIGRATION TO DIGITAL

Digital radio services not only provide better battery life, sound quality, and inherent signal security than analog but also offer spectrum efficiencies and flexible platforms



COST-OPTIMIZED DIGITAL TECHNOLOGIES

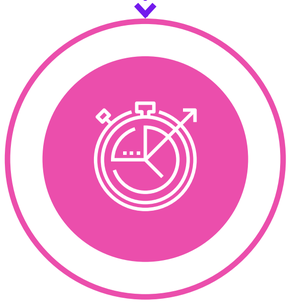
Cost-optimized digital technologies, such as DMR and PDT, have been positioned as a potential replacement for analog radios in systems that can be satisfied by lower-end digital solutions

INTEROPERABILITY AND INTEGRATION

Seamless interworking with legacy public technologies facilitates a smooth evolution path with integration with other applications in the ecosystem such as command-and-control rooms

CRITICAL BROADBAND

LTE and 5G will provide reliable high-speed, data-centric multimedia solutions in addition to critical voice communications



AN EVOLVING COMPETITIVE LANDSCAPE

Traditionally considered a niche market, dominated by players such as Motorola Solutions, Airbus SLC, and L3Harris, this market is witnessing the entrance of service providers, broadband manufacturers, and software application vendors, transforming business models and the capabilities available

SOURCE: OMDIA

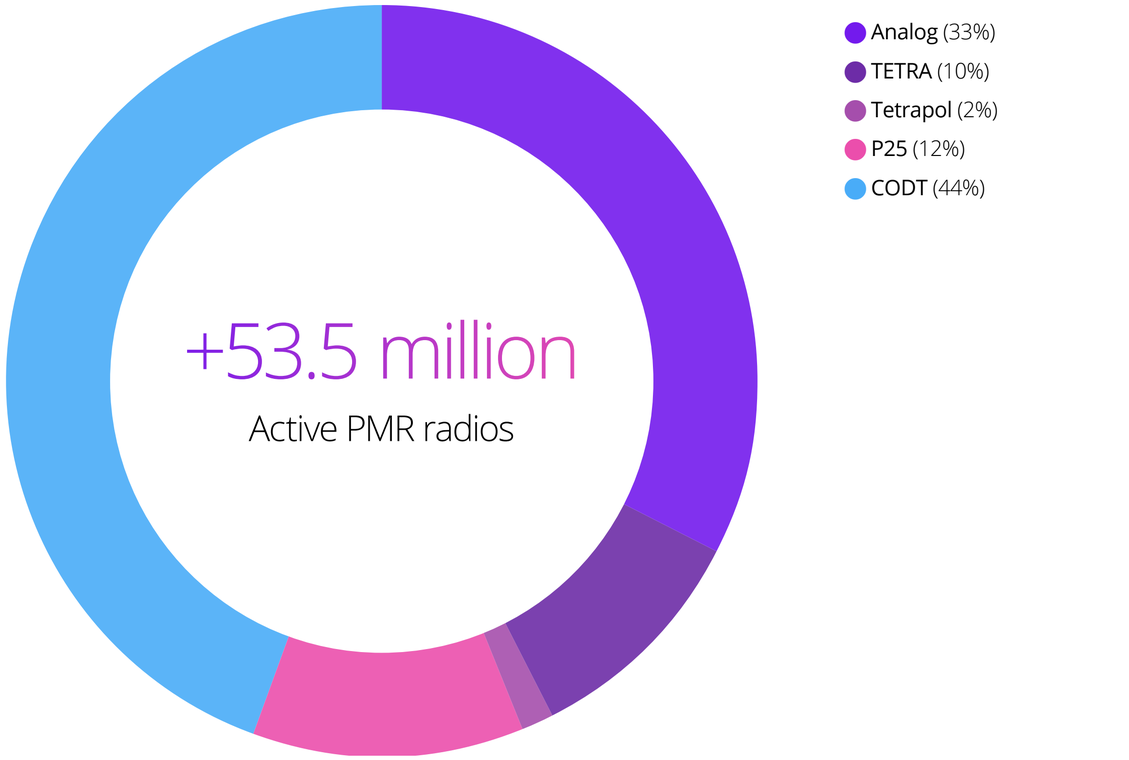
An overview of incumbent critical communication technologies addressing public safety needs

For decades, MCX systems have leveraged narrowband frequency spectrum and focused on providing reliable, secure services to support essential voice communication needs in case of emergency. These narrowband PMR systems have been developed and deployed globally to address the demanding voice requirements of mission-critical user groups.

The PMR landscape includes a variety of protocols, from legacy analog systems to digital high-end systems such as TETRA and APCO Project 25 (P.25) to more cost-optimized digital technologies such as digital mobile radio (DMR) and Police Digital Trunking (PDT).

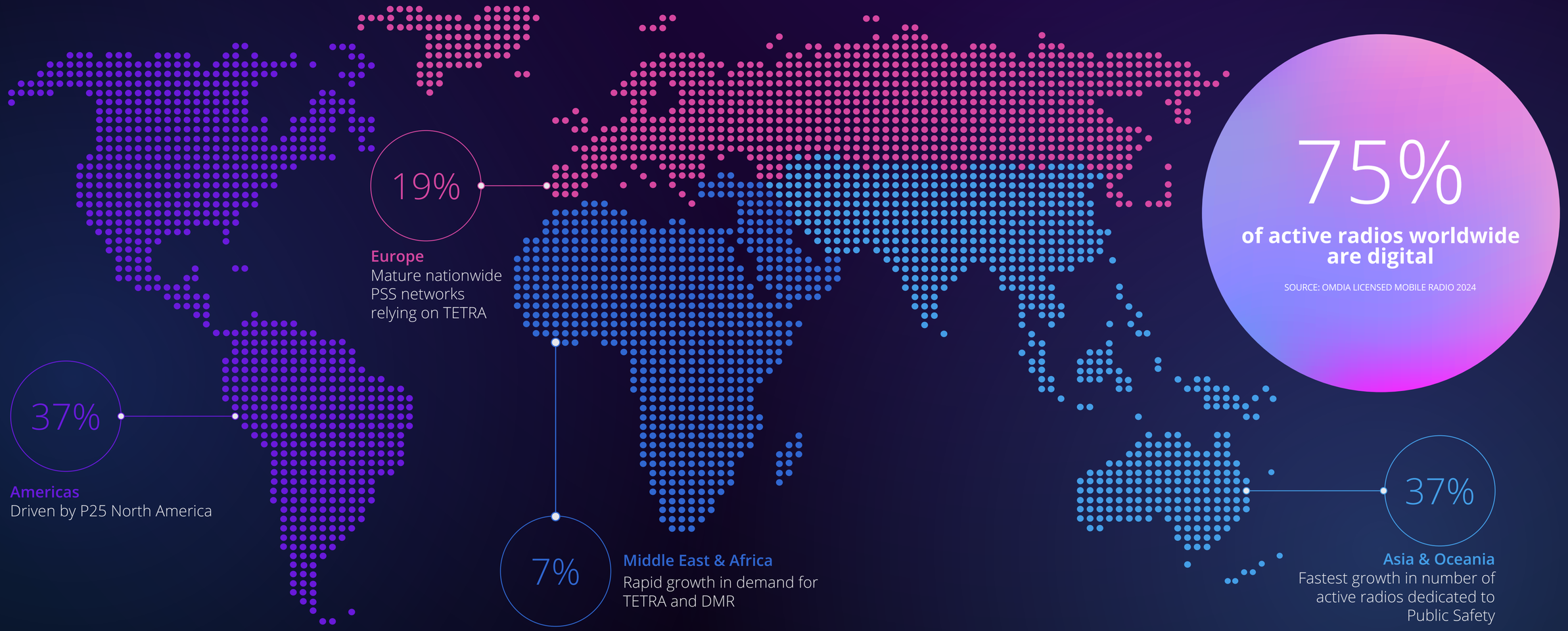
What sets these PMR systems apart is their ability to provide high-quality voice communication even in extreme situations where commercial networks might fail. Their reliability and resilience make them crucial for ensuring effective communication during critical emergencies, solidifying their role as a vital component in public safety operations

Global installed base, private mobile radio



SOURCE: OMDIA

What's happening around the world with LMR (IB)?



75%

of active radios worldwide are digital

SOURCE: OMDIA LICENSED MOBILE RADIO 2024

SOURCE: OMDIA

A natural evolution to broadband to bridge the gaps

Despite their incredible reliability for voice communication, narrowband PMR systems have limitations when it comes to supporting data transmissions. This becomes increasingly problematic as the needs of first responders evolve to include more multimedia capabilities. Public safety agencies need advanced solutions that can match the reliability of PMR systems while expanding their data-handling capabilities to meet the needs of modern emergency response operations. The evolution to mission-critical broadband technology is far more than a mere technology upgrade: it represents a fundamental shift in how public safety agencies will operate. By enabling a suite of powerful new capabilities, critical broadband unlocks a host of benefits that will transform emergency response and elevate public safety operations to new levels of efficiency and effectiveness to save lives.

What is more, by offering dedicated resources, private cellular networks ensure reliable and timely communications even under the most challenging circumstances. A reliable, efficient, and secure public safety communications system is beneficial not only to first responders but to society as a whole.

ENHANCED SAFETY

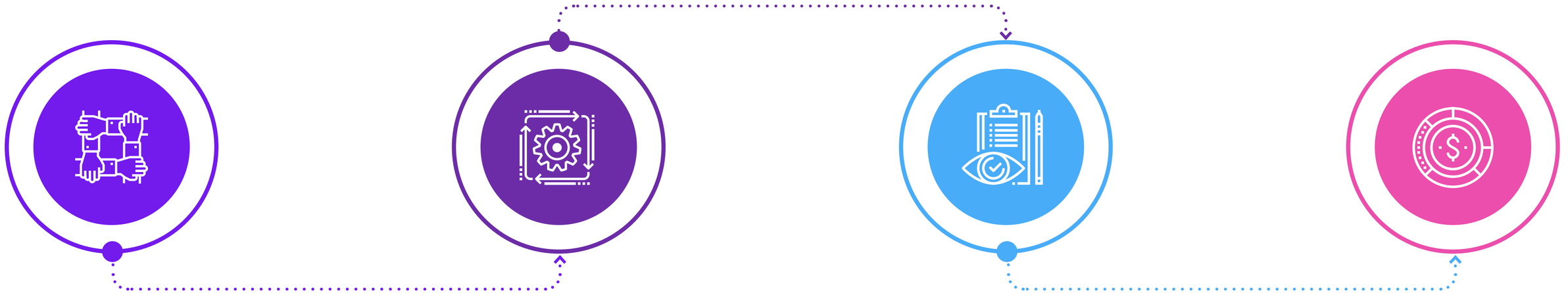
This represents the most direct impact of a reliable, robust critical private cellular network, improving safety in various aspects:

- Crime reduction through effective operations
- Save lives as a direct result of the effectiveness of the response
- Reduced mortality of emergency responders thanks to their improved situational awareness.

SERVICE CONTINUITY

Some studies estimate that a 5% reduction in service availability could potentially generate a socioeconomic cost of over €23.3bn, encompassing 832,000 interventions that could be at risk.

A reliable private cellular network offers coverage reliability, capacity support, and service continuity, guaranteeing the quality of communications services even under the toughest conditions.



OPERATIONAL EFFICIENCY

An improvement in response efficiency that results in better operations by leveraging accurate, real-time data between command-and-control rooms and the frontline emergency response team.

Enhanced operational efficiency is based on collaborative responses because of the enablement of multi-agency sharing.

ECONOMIC STABILITY

Crime and disasters can damage national economic performance. However, if handled efficiently, they become less of a drain on a nation's economy.

Additionally, strategic design of private networks can optimize national investment and improve resource cost-efficiencies

Critical broadband networks for public safety: From a siloed to a holistic approach

NEW PARADIGM SHIFT: PUBLIC SAFETY MOVING FROM VOICE TO DATA

Governments and public safety agencies around the globe are considering cellular broadband technologies such as LTE and 5G, which promise enhanced mobile broadband and ultra-high reliability, to strengthen their critical networks. Emergency responders need access to up-to-date communication capabilities beyond voice-only services. Omdia forecasts a global 15% CAGR growth for mission-critical LTE devices.

TRANSFORMATION DRIVERS ARE FUELING BROADBAND ADOPTION

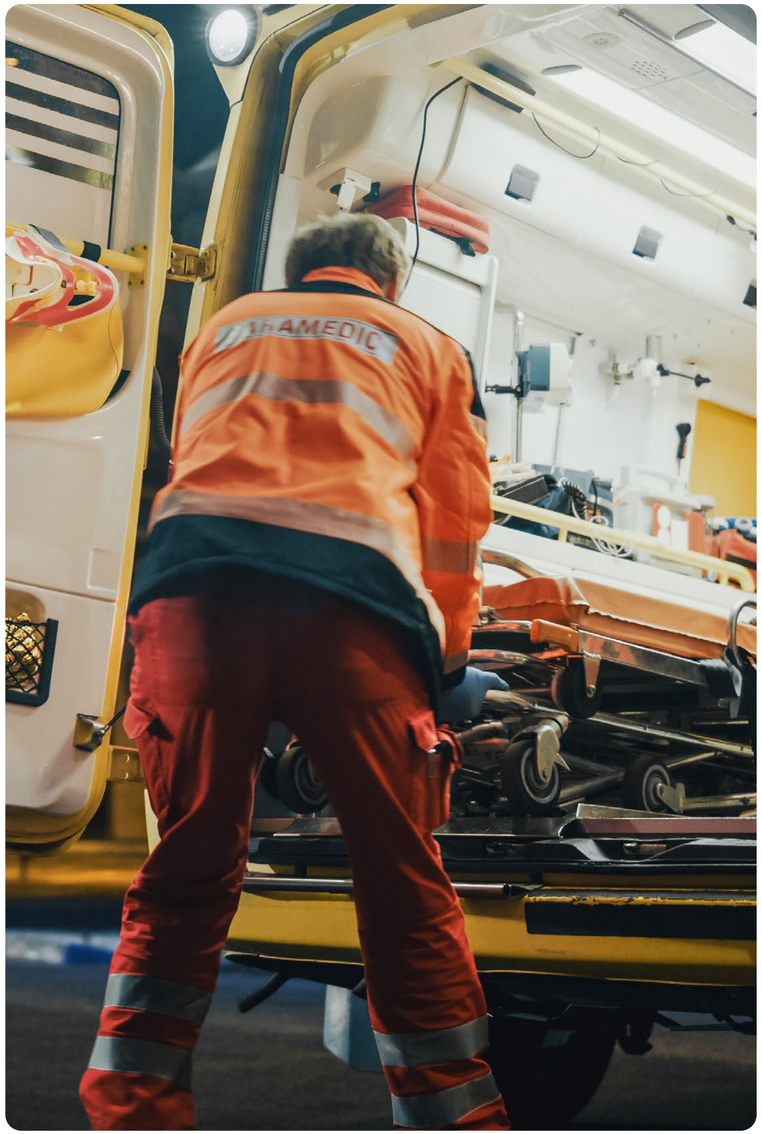
It is by understanding the causes of this shift that public safety agencies and governments can plan and prepare the right decisions to make for their future mission-critical communication networks. The key user requirements that can only be addressed by broadband technology are as follows:

Leveraging multimedia data: Voice communication remains crucial for mission execution, but mobile broadband now enables field-based data functions. This includes incident logging, report filing, and accessing information about suspects, scenes, and hazards. These data services are expected to grow significantly, with a projected 37% CAGR in Europe for the installed base of module and data card connectivity.

Maximizing situational awareness: Command-and-control Rooms (CCRs) are the center of an organization's operation. They often must make critical decisions based on analysis of accurate field information. LTE and 5G technologies enable real-time transmission from diverse data sources including sensors, body-worn cameras, and drones. This improved information flow enhances accuracy of decision-making and can make response faster and more effective.

Enabling cross-agency collaboration: Open 3GPP standards for LTE and 5G facilitate seamless information sharing and cooperation between different agencies. This interoperability overcomes the limitations of siloed PMR networks, significantly improving the success rate of emergency response.

Reducing costs: The adoption of critical broadband technology offers substantial cost savings. Global open standards and a competitive ecosystem drive innovation and cost-efficiency. The flexibility of 3GPP-based broadband technologies allows many public safety agencies and critical enterprises to collaborate while meeting stringent requirements.



The gains for public safety agencies deploying private LTE/5G networks

Public safety agencies have always had a reliance of private wireless communications. Their journey toward the adoption of critical broadband capabilities is driven by the demand for more effective and adaptable technology, but it should not come at the expense of the reliability, security, or flexibility of the network. This is where private LTE and 5G networks can really address the needs of public safety agencies and critical government networks.

These next-generation private cellular networks provide agencies with unprecedented control and flexibility, allowing them to customize and secure their communications to meet the unique, stringent requirements of emergency response. Agencies will gain access to new, mission-critical use cases—such as real-time video feeds and IoT integration—that significantly enhance their operational capabilities, enabling faster, more informed, and more coordinated responses when every second counts.

Governments and public safety agencies across the world are starting their journey toward critical broadband adoption with LTE. One key advantage is that LTE is a future-proof standard-based technology with a large ecosystem of partners.

Schematic representation of the main Public Safety communication requirements

SOURCE: OMDIA

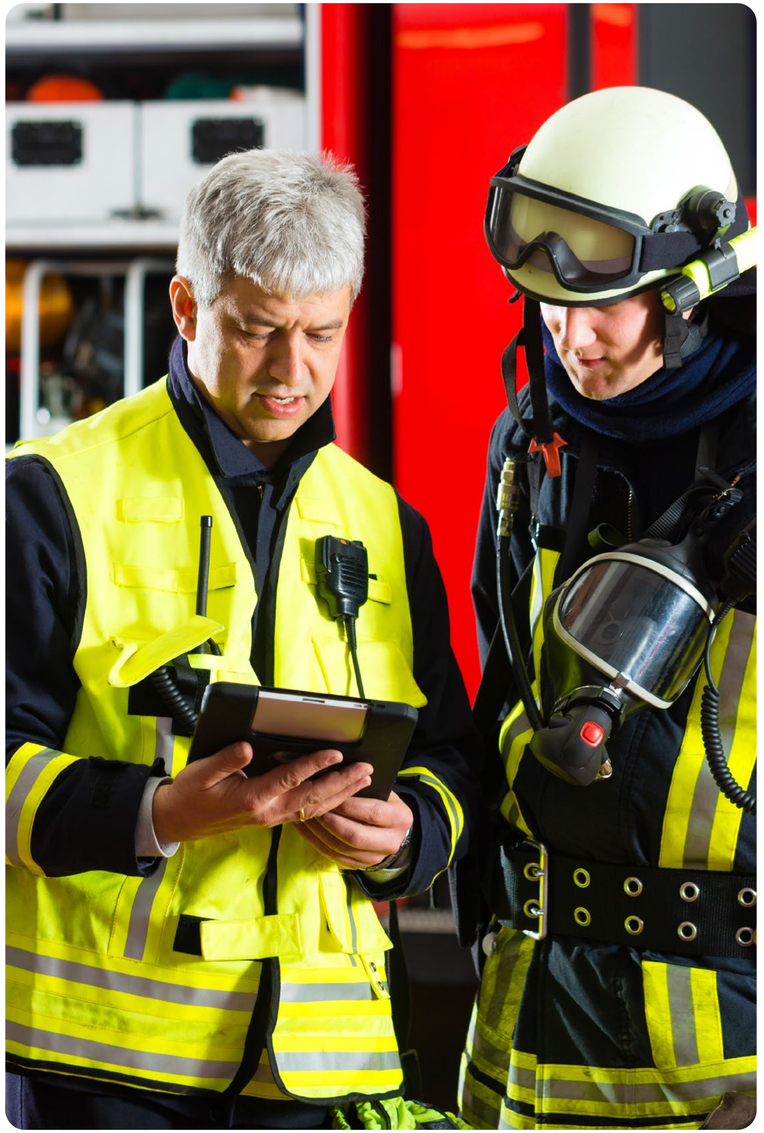
PREPARED FOR THE FUTURE: THE PATH TO 5G

The next step beyond LTE is 5G, and it is now in operation in several advanced networks around the world. The initial impact of 5G on public safety networks is beginning: there have been official government announcements in the US and Sweden with commitments to deploy critical 5G networks for public safety.

To understand why, it is useful to look at the essential characteristics of 5G technology. Academic and industry efforts have produced a next-generation wireless air interface that builds on the LTE network and brings the following:

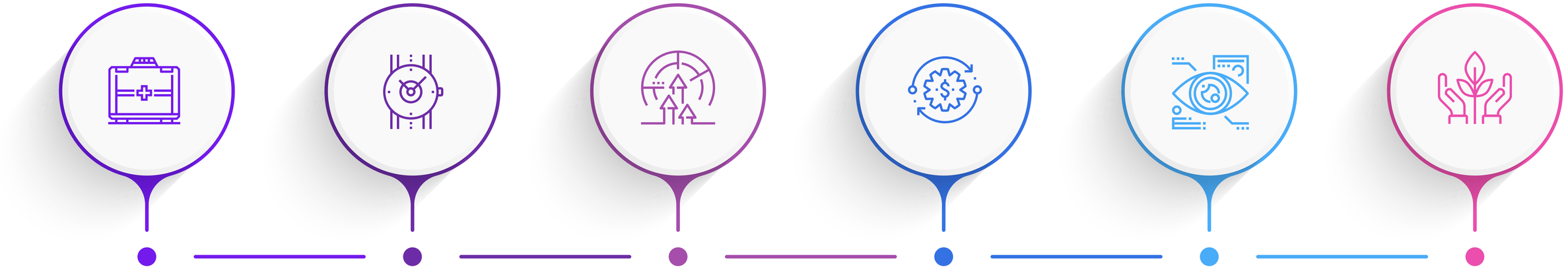
- **Enhanced mobile broadband:** This results in throughput that approaches 10Gbps, a sharp contrast to lower-band LTE performance that hits a limit of 1Gbps.
- **Future-proof radio air interface:** The radio air interface supports a wide variety of digital streams.
- **Ultra-reliability and low-latency communications (URLLC):** 5G NR drives down the latency of transmissions across the air interface. Along with improvements in latency, 5G provides mechanisms that support ultra-reliable transmissions that go beyond LTE's levels of reliability.
- **Energy efficiency:** The 5G NR air interface is designed to enable reduced power in portions of the grid where transmissions are not in progress. These efficiencies reduce the cost to operate and help 5G devices save battery life.
- **Promise of massive machine-type communications:** 5G technology promises massive connectivity and support for massive machine-type communications (mMTC), enabling the seamless integration of millions of connected devices
- **Unified communication layer:** Because 5G will bring more capacity, it will serve even more use cases. Currently, having multiple networks (e.g., TETRA, PLC, etc.) leads to high capex and opex and a need for experts for each network, backup options for power, troubleshooting, cybersecurity experts, and so on.

The benefits of having a large ecosystem should also not be underestimated. There is a wide array of devices available for cellular technology. Additionally, 3GPP is increasingly liaising with vertical industries on the development of new standards. This means that public safety as a whole can help shape the future of cellular in line with its needs and priorities.



THE OVERALL BENEFITS UNLOCKED BY PRIVATE CELLULAR NETWORKS

There are many drivers for governments to deploy a private cellular network. Above all, first responders aim to deploy a network to better handle, collect, and process multimedia data and to enable collaboration and coordination among public safety agencies. The public safety agency of the future must have better visibility and control capabilities across its whole distributed footprint, and to do so it must collect and handle data in a reliable and effective way.



Improved first-responder safety

The biggest driver for enhanced critical broadband connectivity in public safety agencies is its direct impact on the safety of first responders.

Law enforcement and fire and rescue agencies aim to use data extracted from video and other sensors to be able to swiftly identify possible threats to their agents in the field.

Shorter crisis response time

Response time is a parameter of paramount importance for public protection and disaster relief agencies. Public safety agencies and decision makers strongly believe enhancement of situational awareness will result in direct improvements in early threat detection and faster reaction in the event of a crisis.

Operations efficiency or productivity gains

Governments and public safety agencies are seeing, or expecting to see, benefits to their operational efficiency beyond crisis response. Post-incident management and evidence management will benefit from multimedia supported by broadband connectivity integrated into command-and-control rooms, and analytics will improve the pattern analysis for threat prediction.

Cost saving

The adoption of 5G and LTE will effectively increase the return on investment made by governments and public safety agencies enhancing their critical communication networks.

Greater insights into operation status

One important driver for the adoption of private networks, in addition to broadband connectivity for safe cities, is the need for enhanced visibility into existing operations, enabling improved process quality and efficient strategies.

Improved sustainability

Although most enterprises have environmental sustainability targets, governments are not currently setting these for their public safety operations. Omdia believes this is still a goal that will permeate all public decisions. Many governments are including sustainability goals as part of longer-term national critical infrastructure plans that have yet to be prioritized.

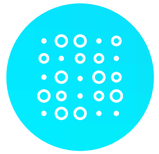
CRITICAL BROADBAND ENABLES INNOVATIVE USE CASES

Broadband technology creates unprecedented possibilities for public safety agencies to incorporate into their toolbox and response procedures. Empowering emergency responders with advanced, data-driven tools is something that was unimaginable with traditional narrowband systems. By leveraging the high-speed, high-capacity, and low-latency capabilities of 4G and 5G networks, public safety agencies can now implement innovative applications that ensure the highest quality of service, even in critical, high-demand scenarios. These new capabilities enhance situational awareness, facilitate faster and more effective decision-making, and improve operational efficiency, ultimately enabling responders to save more lives and protect communities with greater precision and reliability. The following use cases showcase the transformative impact of broadband on public safety operations, highlighting how each application elevates the speed, safety, and effectiveness of emergency response in real time.

Push-to-video: Push-to-video allows responders to share live video streams instantly, giving command centers real-time visuals to support coordinated decision-making.

Status message: Simple status messages provide quick updates on responder availability or incident status, ensuring command centers are informed with minimal data bandwidth.

Location sharing: Real-time location sharing tracks responder positions, enhancing situational awareness and enabling efficient resource deployment during emergencies.



Database check: Automated number plate recognition (ANPR) or other database checks allow responders to instantly access critical information such as vehicle or suspect details, directly in the field.

File sharing: Secure file sharing enables access to essential documents such as building layouts or medical records, improving on-scene decision-making and response accuracy.

Asset tracking: Continuous asset tracking ensures visibility of critical equipment and vehicles, optimizing resource allocation and reducing response times.

Live monitoring via body-worn camera: Body-worn cameras capture live recordings, documenting incidents for accountability and providing visual context to command centers during emergencies.

Drones: Drones provide aerial views, conduct surveillance, and support search-and-rescue missions, gathering valuable data quickly and safely from above.

Deployment options: What governments and agencies need to know to deploy a private LTE/5G network

When adoption of cellular technology is under consideration, different deployment options are available for public safety networks:

Commercial deployment – private network fully dependent on the public network: Public safety agencies rely on a partner mobile network operator (MNO) to deliver connectivity services through the macro radio access network (RAN) and public core. The public safety organization gets access to and pays for the service by using specific access point names (APNs). This will, however, provide limited service KPI differentiation. This may be more cost-effective since it is leveraging existing infrastructure. However, public safety agencies relying on public network services may face limitations in their ability to prioritize the use of resources (quality of service, priority, and preemption) and tailor operations to their needs for coverage, backup power, and so on.

Hybrid network: This is a network with some infrastructure dedicated to the public safety network and some that is shared with the MNO's public network. The public RAN will deliver coverage and capacity enhanced by private RAN to avoid coverage holes or outages. Devices can also access services, such as voice calls and data sessions, on the public network.

Shared network: Governments pay MNOs for connectivity by providing uniquely defined APNs, which will enable the public safety devices to be differentiated within the network from all other consumer devices and smartphones. This, in essence, creates a virtual network, similar to how mobile virtual network operators (MVNOs) operate, where the devices on that network are differentiated from those on the host communications service provider (CSP) network.

Fully dedicated RAN and core exclusively for public safety agencies: This is likely the most expensive option but also the one that more than any other can be tailored to serve all the needs of the public safety agencies. Governments deploy their own RAN and core, which will required initial capex investment. The network will be fully isolated from the public network, and though the public safety organization may seek support from systems integrators, the network will be under its control.

COMMERCIAL

Suitable for governments without dedicated spectrum forced to rely on commercial MNO resources through partnerships

Quality of service, priority, and preemption are mandatory to support public safety users

Security and performance concerns are ideal for initial proofs of concept and early deployments

SHARED

Suitable for governments with spectrum but low budget resources

Models including MOCN and S-MVNO belong in this category

Concerns about operational costs and coverage reliability

HYBRID

Suitable for governments with enough budget to address coverage concerns with their own dedicated infrastructure

Fallback mechanisms between dedicated and commercial resources

FULLY DEDICATED

Ideal case for reliability and performance

Dedicated infrastructure for mission-critical users with the highest investment level required

Depending on the scale of the network

National critical communications networks

Private network deployments

CHALLENGES: INNOVATION IS NOT A SIMPLE PATH

Despite the surging interest in private broadband networks, there is a list of factors and challenges that need to be considered by governments and public safety agencies that are planning to replace their proven PMR technology with a more powerful but unfamiliar alternative.

The shift from trusted, purpose-built, resilient PMR technology to an unproven MC-PTT service built on private LTE can raise some technology concerns:

Spectrum availability: Spectrum availability and regulations differ depending on country and region. Spectrum can be obtained from the regulator or from an MNO. Given the nationwide coverage needs of the emergency responders, it is wise for public safety agencies to secure some low-bandwidth spectrum, ideally sub-1GHz. This can then be complemented with higher-bandwidth spectrum for additional capacity. The amount of spectrum available also influences what services first responders can enable.

Coverage limitations: Ubiquitous and uninterrupted network coverage is a key element of mission-critical networks. Public safety requires 95% in-building coverage; however, most cellular providers find this unachievable. To overcome this major challenge, supportive coverage alternatives should be put in place (tactical hubs, network on wheels, backpack networks, or satellite connectivity are some of the solutions that different users are evaluating).

Direct-mode limitations: The low output power available to handheld LTE devices creates a barrier for useful applications of the standardized 3GPP proximity services. Direct mode remains a fundamental requirement, so industry and government will need to develop alternatives that work. In TETRA technology, the direct-mode back-to-back option provides a mechanism to communicate during times when network controllers cannot be accessed. Absent a proven LTE ProSe mechanism, national public safety operators cannot shift users to LTE unless an alternative becomes available. The most straightforward approach is to incorporate a PMR technology for local unit-to-unit transmissions in combination with high-bandwidth LTE.

Interworking with legacy radio systems: The 3GPP standards organization has completed standardized interworking functions that allow interoperability between legacy PMR systems and LTE-based MC-PTT. However, technology-specific standardization efforts, such as those needed for TETRA, remain a work in progress. Unfortunately, 3GPP's work will not be ready before several major systems begin deploying MC-PTT networks. This gap means that each vendor will probably take a proprietary approach to solving the problem.

End-to-end integration with command-and-control rooms with supported communication between first responders in the field and their dispatch center and CCR to streamline incident management workflows.

An overview of technical features needed by public safety agencies

HOW CELLULAR TECHNOLOGY WILL DELIVER ON THE PUBLIC SAFETY USERS' REQUIREMENTS

Trust

For public safety agencies and first responders, communication technology continuously acts as their lifeline during an emergency response. Therefore, trust in their communication system is paramount. This can only be achieved by systems that enable reliable, secure, and proven solutions that will serve first responders under any circumstances, including in the most challenging environments:

- Broadband solution providers have delivered reliable communication services to millions of CSP consumers around the world. Given their complex requirements, the solution vendors must be trusted to provide secure and reliable services 24/7, complying with market regulations.
- The public safety organizations must ensure they partner with a core solution vendor that delivers the same level of trust and security as they deliver to the large service providers.
- A 5G core leverages the service-based architecture (SBA), and as part of the new modern ecosystem of network functions, 5G core benefits from the Security Edge Protection Proxy (SEPP) network function, which sits at the edge of the network and delivers protection against external attacks.

Longevity

The trends shaping the public safety organizations are emerging now, but they will not end any time soon, given the assets are expected to last more than 10 years. The public safety organization's communication network needs to be able to continue to support and evolve alongside the growth of these trends:

- One of the major concerns that public safety organizations have is the need to future-proof their investments, given that many expect the lifespan of these networks to be more than 20 years. Networks and software solutions evolve continuously over time, and without planned platform upgrades, the networks can become obsolete and will not be able to deliver communication based on the 3GPP specifications between the network and devices or deliver on the latest features that 5G or, later, 6G will bring.
- Because the 5G core is built using an SBA, the network operator is able to easily modify the network functions present (mutability) and ensure the right network function elements are present to deliver the necessary functionalities.

Interoperability

Public safety communications are complex ecosystems, currently supported mainly by narrowband PMR systems such as TETRA and P25. It is critical for an effective emergency response that any new solution can interoperate with legacy technologies and command-and-control room and dispatcher systems and can enable collaboration across agencies and solutions. The need for interoperability will remain open throughout the whole lifespan of the network as innovative solutions are adopted:

Simple operations

Though the public safety organizations have networking teams and experts that can deal with network management, simplicity of operations is essential to ease the workload of these teams and thus enable them to focus on the utility's core business:

- Modern networks have thousands of parameters to maintain. Once these were optimized using manual activities, but in the 5G era, the number of parameters will be several orders of magnitude higher, and manual changes to parameters will no longer scale given the complexity of the problem.
- Public safety organizations will require a core network solution that leverages the state-of-the-art automation processes that come with modern cloud-native solutions to reduce not only repetitive manual-intensive tasks but also operational costs.
- Network solution must also function without errors, keeping service interruptions to a minimum.
- Furthermore, the solution will need to have a reduced footprint in order to save on both cabinet space and power usage requirements.

Optimization

A public safety organization has very specific needs in terms of devices, coverage, resilience, reliability, cost, and scalability. It needs a solution fully tailored to its business to be forward looking in a highly competitive and regulated market:

- Today, management of the total cost of ownership (TCO) is at the top of most service provider organizations' requirements: vendors must leverage all the tools, such as containerization, that cloud-native design brings to better manage the platform's resource requirements and cater for future capacity requirements.
- Network and resource scalability is an important feature of 5G networks. For example, when the devices require higher bandwidth for a specific time, the core network must scale the necessary resources dynamically to deliver those requirements and then scale them down when they are no longer required, releasing the resources to another customer. Only today's cloud-native-based networks are capable of such agility and resource usage optimization.

NOKIA'S PRIVATE WIRELESS SOLUTIONS CAN HELP MEET THE NEEDS OF PUBLIC SAFTY AGENCIES

To cater to public safety agencies' unique requirements, Nokia has developed its Core Enterprise Solution, providing the foundational infrastructure for private LTE and 5G wireless networks.

Agencies have flexible deployment options. They can start with an LTE network that is fully upgradable to 5G, deploy both 4G and 5G simultaneously, or choose to implement a dedicated 5G-only network from the outset.

This solution is specifically designed to meet critical public safety needs—delivering trust, longevity, and interoperability. Additionally, it simplifies operational management and allows for optimized network performance.

Case study

EMPOWERING PUBLIC SAFETY WITH PRIVATE CELLULAR NETWORKS

THE BACKGROUND

Around the world, governments are increasingly exploring the potential of mobile broadband to enhance public safety communications. The need for more reliable, interoperable, and data-rich communication systems has become paramount in the face of more complex emergency scenarios, growing demands on first responders, and the evolving threat landscape.

In response, government and public safety agencies globally are initiating programs to evaluate and deploy dedicated or hybrid broadband networks tailored to their unique operational requirements. These efforts aim to transform national critical communication systems and future-proof communications, improve situational awareness, and foster better coordination across their Emergency Service Organizations (ESOs).

One such example from the Asia-Pacific region involves a government initiative to transform its critical communications systems by piloting a mission-critical broadband solution. This initiative was structured as a proof-of-concept (PoC) to assess how critical broadband and private cellular networks, enabling multimedia broadband services.

TECHNICAL OVERVIEW: PHASED APPROACH

The PoC brought together a diverse ecosystem of key players, each contributing their expertise to ensure the project's success. A private 4G & 5G core was set up to anchor the critical broadband network and dedicated base stations. Local Communication Service Providers (CSPs) played a pivotal role as the telecommunications operator partners enabling seamless roaming capabilities to extend coverage. The ecosystem of vendors included mission-critical devices, testing tools, deployable solutions like Cells on Wheels (COWs), satellite backhaul systems and interworking system with legacy LMR systems

This collaboration highlighted how public-private partnerships drive innovation for public safety, showcasing how technology manufacturers, telcos, and solution providers can work in unison to transform emergency service operations. Throughout the PoC, a comprehensive set of test cases were conducted across four phases. Early phases focused on lab-based tests for MCPTT features, QoS, and security, while later phases emphasized field testing for roaming, advanced MCPTT functionality, and live integration with the P.25 system.

PHASE 1

Initially, the lab setup integrated the core network with basic radio access network (RAN) equipment to simulate public safety scenarios. Key tests included validating one-to-one and group Mission-Critical Push-to-Talk (MCPTT) voice communications, ensuring correct implementation of Quality of Service (QoS) protection and pre-emption mechanisms, and verifying end-to-end encryption for secure communications.

PHASE 2

Phase 2 expanded the setup to a live network environment by integrating into the local CSP's infrastructure. Dedicated public safety RAN nodes were deployed to support the private core. During this phase, the solution successfully demonstrated its ability to handle Mission-Critical Voice and Video (MCVideo) applications, including high-quality video calls and real-time streaming. The QoS policies were validated to ensure that public safety traffic was prioritized during network congestion.

PHASE 3

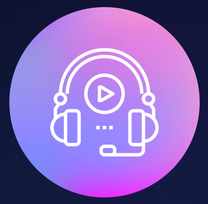
Phase 3 focus shifted to enabling seamless roaming between the dedicated network and local operator networks. The implementation of both Multi-Operator Radio Access Network (MORAN) and Multi-Operator Core Network (MOCN) configurations allowed shared access to resources. Roaming tests were conducted across different dedicated sites and five roaming sites managed by local CSPs. These tests confirmed that first responders could maintain reliable connectivity with priority and pre-emption capabilities across different networks.

PHASE 4

The final phase involved achieving seamless interworking between the new broadband system and the existing P25 LMR network. This was accomplished by integrating a partner Interworking Function (IWF). Testing focused on enabling real-time communication between users on LMR and LTE/5G networks. Emergency group calls, push-to-talk capabilities, and comprehensive security mechanisms were validated to ensure interoperability without compromising mission-critical performance.

KEY TEST FOCUS AREAS AND RESULTS

The PoC validated key technical and operational capabilities essential for a broadband network supporting public safety communications. Among the tested features:



Mission-Critical Voice Services

Security and Resilience

Multimedia and Real-Time Situational Awareness

Tactical Coverage Solutions

QoS and Traffic Prioritization

Seamless Roaming

Interoperability with LMR

CONCLUSION: KEY TAKEAWAYS FROM A SUCCESSFUL POC

These efforts successfully demonstrated the feasibility of private cellular networks for public safety communications:

- **Validation of Critical Broadband Deployment:** The PoC successfully demonstrated the deployment of a reliable broadband network tailored to the unique needs of public safety users, ensuring secure, prioritized, and mission-critical connectivity.
- **Feasibility of Advanced Mission-Critical Features:** The project validated the capability to go beyond voice communications, showcasing Mission-Critical Push-to-Talk (MCPTT), data exchange, high-quality video calls, QoS prioritization, and robust security mechanisms across diverse operational scenarios.
- **Implementation of Coverage Reliability Models:** Innovative solutions and architectures were tested to ensure consistent network performance and coverage reliability in both remote and critical conditions.
- **Seamless Integration with Multiple Architectures and Interworking with LMR Systems:** The PoC demonstrated smooth integration with telco networks using integration with MORAN/MOCN configurations, as well as seamless roaming across networks, and interworking with legacy P25 systems, enabling interoperability and future-ready flexibility.

The successful results of this proof of concept confirmed the feasibility of implementing a nationwide broadband solution, laying a strong foundation to transform national emergency service operations and equip first responders with advanced broadband communication capabilities.

Appendix

About

Nokia

At Nokia, we create technology that helps the world act together.

As a trusted partner for critical networks, we are committed to innovation and technology leadership across mobile, fixed and cloud networks. We create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Adhering to the highest standards of integrity and security, we help build the capabilities needed for a more productive, sustainable and inclusive world.

Nokia
Nokia

Omdia

Omdia, part of Informa TechTarget, Inc. (Nasdaq: TTGT), is a global analyst and advisory leader that helps you connect the dots across the technology ecosystem.

We combine the expertise of more than 400 analysts across the entire technology spectrum, covering 150 markets. We publish over 3,000 research reports annually, reaching more than 14,000 subscribers, and cover thousands of technology, media, and telecommunications companies.

Our exhaustive intelligence and deep technology expertise enable us to uncover actionable insights that help our customers connect the dots in today's constantly evolving technology environment and empower them to improve their businesses – today and tomorrow.

The Omdia team of 400+ analysts and consultants are located across the globe

Americas

Argentina
Brazil
Canada
United States

Asia-Pacific

Australia
China
India
Japan
Malaysia
Singapore
South Korea
Taiwan

Europe, Middle East, Africa

Denmark
France
Germany
Italy
Kenya
Netherlands
South Africa
Spain
Sweden
United Arab Emirates
United Kingdom

Omdia

E insights@omdia.com
E consulting@omdia.com
W omdia.com

OmdiaHQ
Omdia

Citation Policy

Request external citation and usage of Omdia research and data via citations@omdia.com

Authors

Ildefonso de la Cruz Morales
Senior Principal Analyst,
Critical Communications
askananalyst@omdia.com

Pablo Tomasi
Principal Analyst, Private Networks
askananalyst@omdia.com

Roberto Kompany
Principal Analyst, Mobile Infrastructure
askananalyst@omdia.com