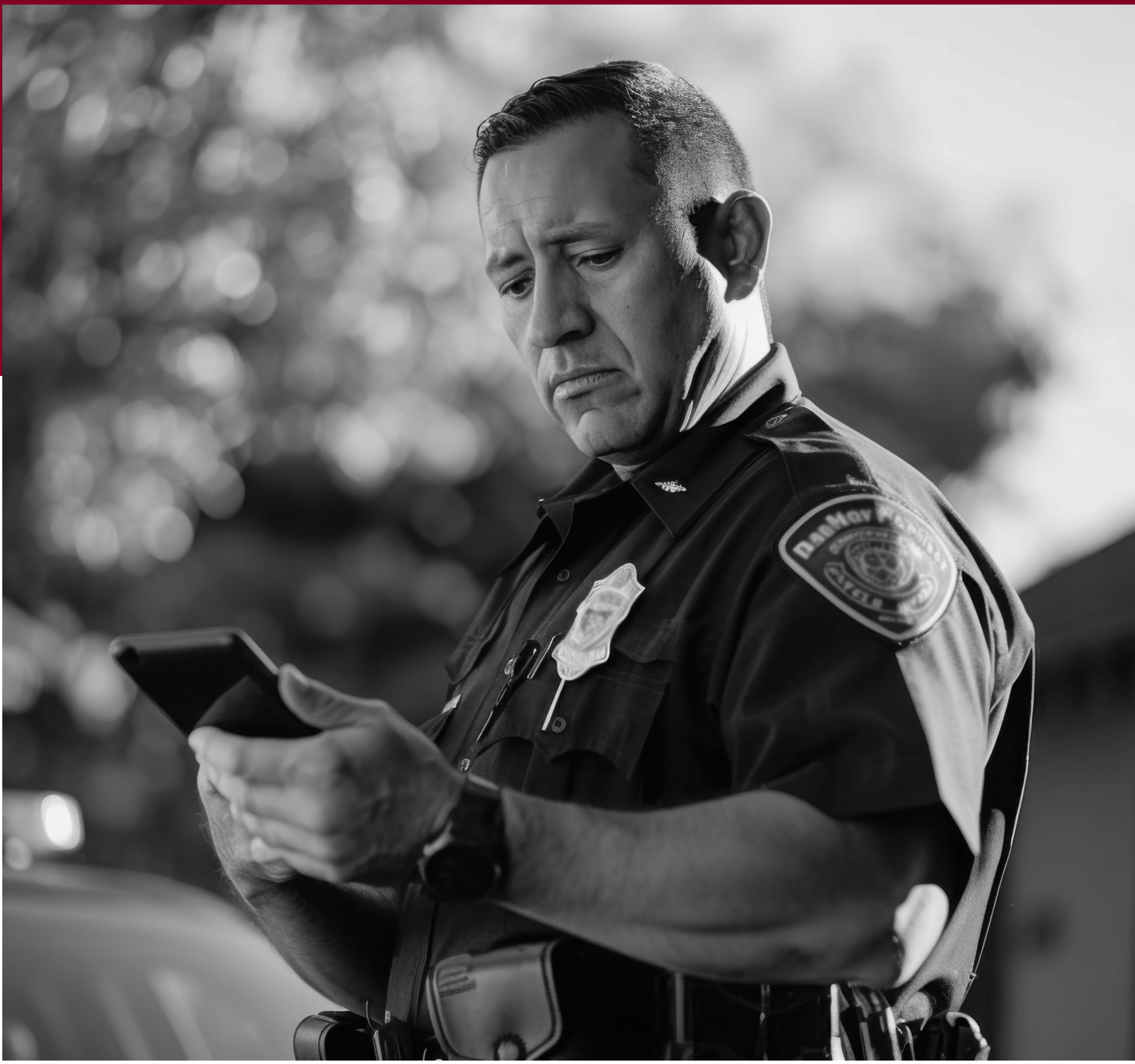
WHITE PAPER

Convergence Of Mission Critical LMR Systems with Private 5G Network



Abstract

This white paper serves as a comprehensive guide for public safety agencies embarking on the convergence journey of their existing mission critical LMR systems with 3GPP Mission Critical system empowered by Private 5G. It provides a vision for coexistence between current LMR systems and the evolving private 5G mission critical system. It shows the potential capabilities of mission critical services with private 5G and why we think it will revolutionize public safety infrastructure.

This synergy between LMR and 5G represents a forward-thinking approach that builds upon the strengths of existing infrastructure while embracing the possibilities of next-generation communications. It ensures that mission-critical systems remain at the forefront of technological advancement, providing unparalleled support for those who rely on these systems in high-stakes environments.

Introduction

Mission Critical LMR (Land Mobile Radio) Systems are dedicated communication networks essential for time-sensitive operations within public safety agencies. Designed specifically for police, fire departments, emergency medical services, and other critical entities, these systems provide immediate, secure, and reliable voice communication. They serve as the primary infrastructure for emergency response, disaster management, law enforcement activities, and other vital operations, utilizing specialized radios, infrastructure elements such as towers, base stations, and dispatch consoles in command centers.

While LMR systems excel in their core function of voice communication, the integration with 5G technology opens up exciting new possibilities to enhance their capabilities. This integration can address the growing need for high-bandwidth traffic support, enabling advanced use cases that require large data transfers and real-time video traffic. By combining the strengths of LMR with 5G, public safety agencies can access valuable information on demand, significantly improving their ability to serve the public and save lives.

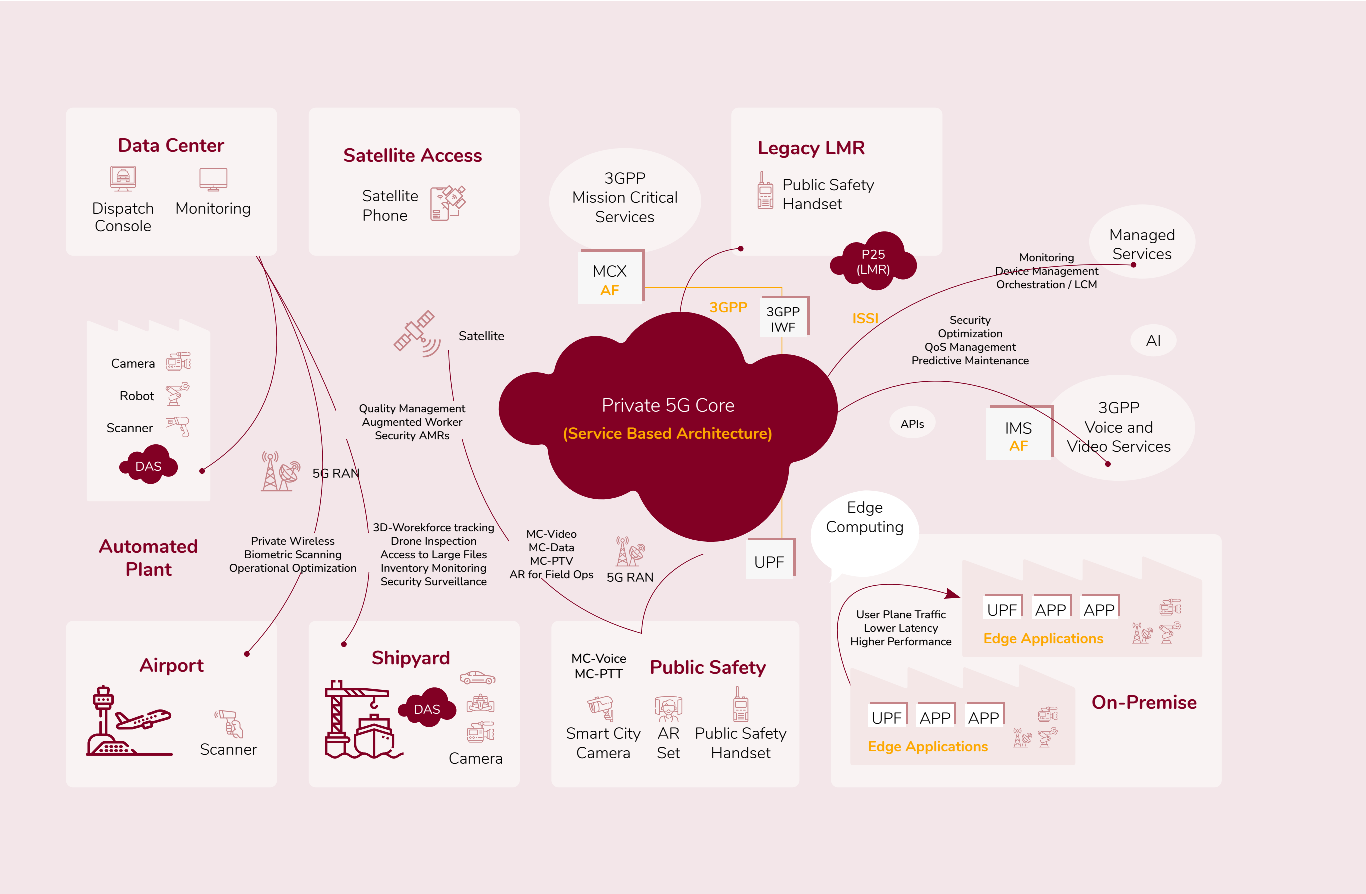
The potential enhancements include live video stream from a police officer, a large video file download, a set of large files with critical data, real-time video from street cameras, a firefighter training with augmented reality (AR) glasses, or drones assisting police in search missions, legacy mission-critical systems cannot offer this capability. The digitization of analog mission-critical LMR to P25 has already enhanced spectral efficiency for voice and facilitated interoperability among different equipment manufacturers. Now, the integration with 3GPP Mission Critical systems and Private 5G can further enhance today's mission-critical services, complementing the existing LMR infrastructure.

This white paper outlines how 3GPP Mission Critical systems and Private 5G can enhance today's mission-critical services and discusses their integration with existing LMR systems. It delves into the various phases required to implement a private 5G-based mission-critical system, emphasizing the critical role of selecting the right Systems Integrator. The paper emphasizes the critical role of selecting the right Systems Integrator, who is essential for defining an effective implementation strategy and executing it efficiently. A competent Integrator ensures that these new technologies not only coexist with but also enhance the existing communication frameworks, creating a seamless and powerful ecosystem for public safety communications.

Enhancements to Mission Critical Systems Powered by 5G

In day-to-day operations, Land Mobile Radio (LMR) systems are well known for their dependability and robustness, supported by redundant infrastructure, they ensure continuous voice communication. While the reliability and security of LMR systems have been key to their success, it is important to recognize that they come with a set of limitations and challenges.

This section illustrates how a 3GPP based mission critical architecture empowered by private 5G technology improves the capabilities of existing systems. The figure below provides a high-level overview of a 3GPP based mission-critical environment serving the needs of public safety, smart cities, airports, shipyards, and automated plants. The architecture comprises a highly scalable and cohesive set of building blocks: 5G serves as an efficient transport service, the MCX (Mission Critical Server) supports all mission-critical applications, the LMR gateway enables interoperability with legacy LMR systems, and the IMS (IP Multimedia Subsystem) manages all voice and video calls.



Improved Scalability and Availability

To grasp the extensive scalability of 5G networks, it's essential to explore some fundamental concepts associated with this technology. All the network functions that provide control and traffic forwarding, as well as all mission-critical applications, are based on microservices. This results in a highly distributed and redundant mission-critical network that can be easily scaled up or down. At the lowest layer of the network is a cloud-native environment that constantly monitors hardware resources, ensuring there is sufficient capacity to host every microservice in the network. Unlike traditional mission-critical systems that depend on purpose-built hardware requiring additional units for redundancy, a private 5G mission-critical network utilizes Common Off-The-Shelf (COTS) hardware, which inherently supports redundancy. In the 5G cloud-native environment, hardware resources (CPU, Memory and Storage) are automatically scaled up or down based on network conditions and real time traffic demands.

Private 5G has been designed to be one of the most flexible, optimal, and adaptable technologies available in the market. From its inception, the implementation of Control and User Plane Separation (CUPS) in private 5G networks was specifically designed to establish a clear distinction between network functions that manage control traffic and those handling user traffic. This allows the strategic placement of network functions to achieve the best possible performance and reliability. For instance, control functions not impacted by latency can be placed in centralized data centers, while those with low delay tolerance can be positioned at the edge of the network closer to the users. From a scalability perspective, control network functions are scaled independently of user-plane network functions, optimizing resource usage. The result is a network environment that manages its own resources and adapts to changes, guaranteeing high availability.

Higher Bandwidth Capacity for Data

By combining LMR's proven reliability with 5G's advanced features, we can create a comprehensive communication ecosystem that preserves crucial voice communications while significantly enhancing data transmission capabilities. This integration allows for the adoption of cutting-edge technologies that can greatly improve situational awareness and support complex operations.

Private 5G networks significantly enhance bandwidth capacity, which is crucial for improving situational awareness and supporting a wide range of mission-critical applications, including massive IoT deployments. With the ability to connect a vast number of devices simultaneously, private 5G networks can handle the extensive data generated by numerous sensors and smart devices integrated across various sectors. This capability is vital in environments where real-time data collection and processing are essential for making informed decisions quickly. Whether it's for monitoring public safety, managing emergency services, or overseeing industrial operations, the robust data throughput and minimal latency of private 5G networks ensure that information is delivered both promptly and reliably. This improved connectivity not only enhances operational efficiency but also improves safety and security, driving better outcomes across all connected systems.

Imagine a scenario involving a large-scale public event in a major city—a situation that requires careful coordination across multiple agencies, including police, fire, and emergency medical services. Private 5G networks enable a command center to utilize real-time video surveillance from hundreds of high-definition camera feeds around the event area. These cameras, along with drones equipped with thermal imaging, provide live updates to the command center, where AI-powered analytics detect potential threats or unusual activities, such as unattended bags or individuals exhibiting suspicious behavior.

Another use case may involve wearable sensors on officers and first responders to stream health and location data back to a command center, ensuring their safety and enabling efficient deployment. Emergency teams can be equipped with AR glasses that display real-time data overlays of building blueprints or hazardous material warnings, directly enhancing on-site situational awareness. The enhanced bandwidth and low latency of the private 5G network ensures seamless video streaming, real-time analytics processing, and uninterrupted communication between the command center and field agents. This network capability transforms how events are monitored and managed, significantly improving response times and safety for both the public and responders.

Wider Range of Frequency Spectrum

The integration of LMR with 5G can help address spectrum challenges and enhance system capabilities:

Spectrum Efficiency: While LMR systems operate effectively in VHF (150-174 MHz) and UHF (421-512 MHz) bands, which offer excellent coverage and voice transmission, 5G technology can complement these by utilizing additional spectrum bands. This integration allows for more efficient use of available frequencies.

Enhanced Bandwidth: 5G's ability to operate across multiple spectrum bands (Low-Band, Mid-Band, and High-Band) can supplement LMR systems, enabling higher bandwidth capacity for advanced mission-critical services such as real-time video surveillance, Push-to-Video, and transmission of high-resolution images alongside voice communication.

Diverse Connectivity Solutions: The multi-band approach of 5G can address various operational needs:

- **Low-Band Spectrum (Sub-1 GHz):** Provides extensive coverage and deep indoor penetration, complementing LMR's strengths in wide-area and rural applications.
- **Mid-Band Spectrum (1-6 GHz):** Offers a balance between coverage and capacity, ideal for urban and suburban areas where higher data throughput is required.
- **High-Band Spectrum (mmWave, above 24 GHz):** Enables ultra-high capacity and low latency for dense urban settings and data-intensive applications.

Future-Proofing: By integrating with 5G, LMR systems can be positioned to meet evolving operational demands without completely overhauling existing infrastructure.

Interoperability: The integration can foster better interoperability between different communication systems, enhancing overall emergency response capabilities.

This synergy between LMR and 5G represents a forward-thinking approach that builds upon the strengths of existing infrastructure while embracing the possibilities of next-generation communications. It ensures that critical communications remain at the forefront of technological advancement, providing unparalleled support for those who rely on these systems in high-stakes environments. The combined system can offer the reliability and coverage of traditional LMR alongside the advanced data capabilities of 5G, creating a more robust and versatile communication network for public safety and emergency response teams.

Vendor Interoperability

Integrating LMR systems with 5G technology presents an exciting opportunity to enhance interoperability and meet the growing demands of modern multi-agency operations

1

Enhanced Interoperability: While LMR systems have made strides in interoperability through protocols like the Inter-RF Sub-System Interface (ISSI) for P25 systems, integrating with 5G can further streamline communication between different agencies and systems. This integration can build upon existing efforts to create a more seamless communication environment.

2

Standardized Protocols: Private 5G and 3GPP mission-critical systems are designed with vendor interoperability as a core principle. By integrating these with P25 standards with LMR, we can create a more unified communication ecosystem that reduces the need for complex customization and integration efforts.

3

Improved Multi-Agency Coordination: The integration of LMR with 5G can facilitate better coordination during joint operations or multi-agency responses. This enhanced interoperability ensures that different agencies can communicate effectively, regardless of their individual systems.

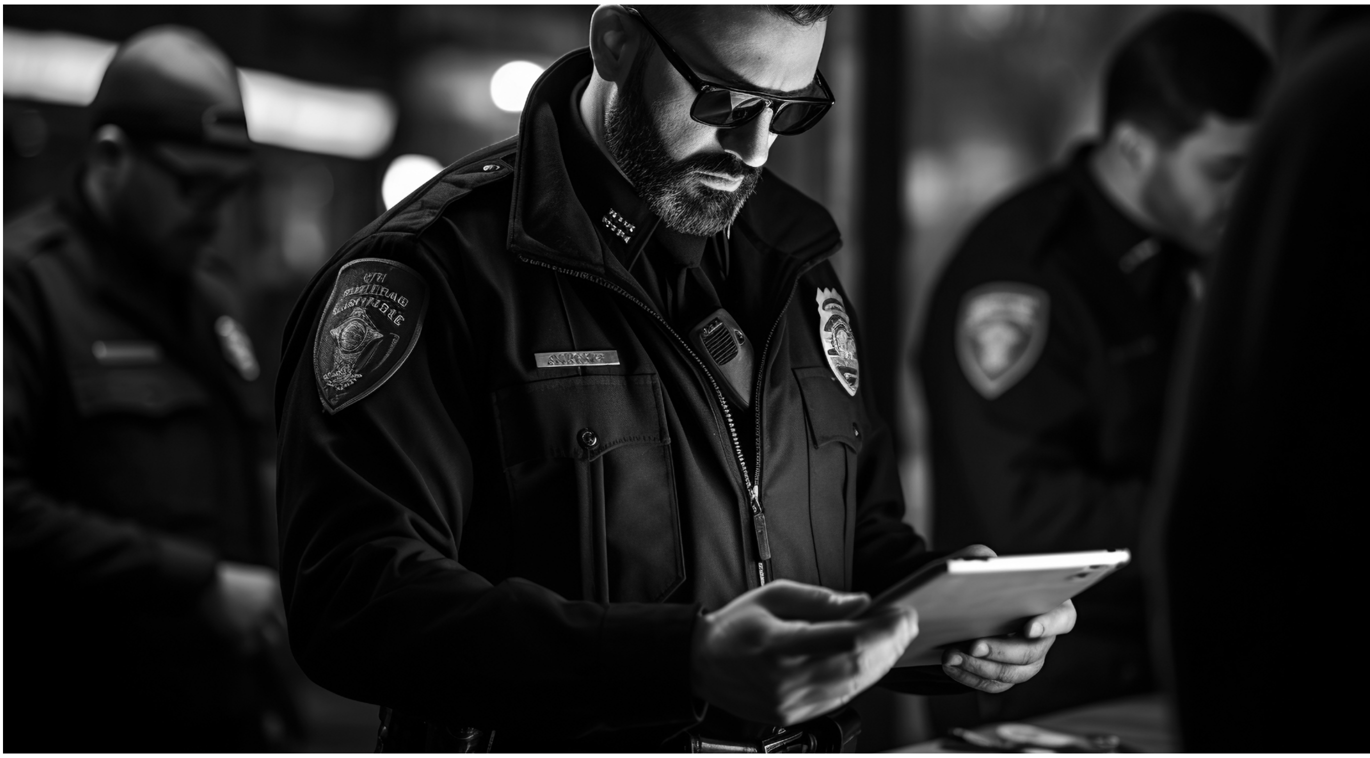
4

Feature Transparency: While LMR systems have made progress in this area, the integration with 3GPP specifications can further extend features across multi-vendor platforms. This ensures that all agencies have access to the same advanced capabilities, enhancing overall operational efficiency.

5

Seamless Communication Continuity: The integration of 5G into the LMR handsets provides a smooth transition between LMR and 5G networks, ensuring uninterrupted communication even as users move between coverage areas or switch between voice and data services.

This synergy between LMR and 5G represents a forward-thinking approach that builds upon the strengths of existing infrastructure while embracing the possibilities of next-generation communications. It ensures that critical communications remain at the forefront of technological advancement, providing unparalleled support for those who rely on these systems in high-stakes environments.



Integration with AI

While traditional LMR systems may have limited interfaces with external systems, integrating with 5G opens up new possibilities. The ability to expose standard REST APIs allows for seamless communication with third-party systems, enabling LMR to leverage advanced capabilities and remain at the forefront of mission-critical communications. With advancements in AI, automation, and data analytics, LMR systems can leverage capabilities such as predictive maintenance, quality of service management, security and threat detection.

One of the key attributes that private 5G brings to the mission-critical landscape, which ensures its relevance for years to come, is its ability to expose standard REST APIs to third-party systems. This capability enables the mission-critical system to share data and real-time events, allowing third-party systems to take appropriate actions based on such data. With this functionality, mission-critical systems can leverage AI, automation and data analytics to optimize network functions and improve reliability. Through continuous data processing, AI identifies and resolves issues like network congestion and signal degradation in real-time, enabling the network to automatically optimize and self-heal, thereby maintaining peak performance.

Predictive maintenance capabilities allow AI to anticipate equipment failures or performance declines by analyzing sensor and device data, enabling proactive repairs that reduce downtime and enhance reliability. AI also enhances quality of service management by monitoring and optimizing network service levels, prioritizing traffic to guarantee low-latency and high-reliability for critical communications, while managing less critical traffic efficiently. Additionally, AI-driven resource management and load balancing ensure optimal resource allocation, preventing resource wastage and ensuring vital applications always have the necessary support. Furthermore, AI enhances security by monitoring network traffic to quickly detect and address potential cyber threats, safeguarding data integrity and confidentiality. Together, these AI-driven capabilities ensure that mission-critical networks are not only robust and secure but also highly adaptive and efficient.

Integration with Non-Terrestrial-Networks (NTN)

One of the challenges faced by traditional wireless technologies is their inability to provide complete coverage. In contrast, 5G is designed as an access-agnostic technology, which includes support for Non-Terrestrial Network (NTN) access to fill any coverage gaps. With 3GPP defining the specifications for interoperability with NTN, 5G has the potential to achieve and guarantee global coverage, transcending the limitations of terrestrial cell towers and extending connectivity across all regions of the Earth, including remote land areas and oceans.

Among the three types of satellites—Geostationary Earth Orbit (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO)—LEO satellites stand out as the most suitable for mission-critical applications, primarily because of their low latency and minimal power requirements for connected devices. LEO satellites achieve latency ranging from 30-50 milliseconds, making them ideal for applications where rapid data transmission is crucial.

Combining 5G and satellite technology provides a robust solution for modern connectivity needs, especially in mission-critical networks. 5G delivers high-speed, low-latency communication within cellular network coverage, significantly improving data transmission rates and response times over previous generations. In contrast, satellite communication excels in extending connectivity to remote, rural, or otherwise inaccessible areas outside the reach of terrestrial networks.

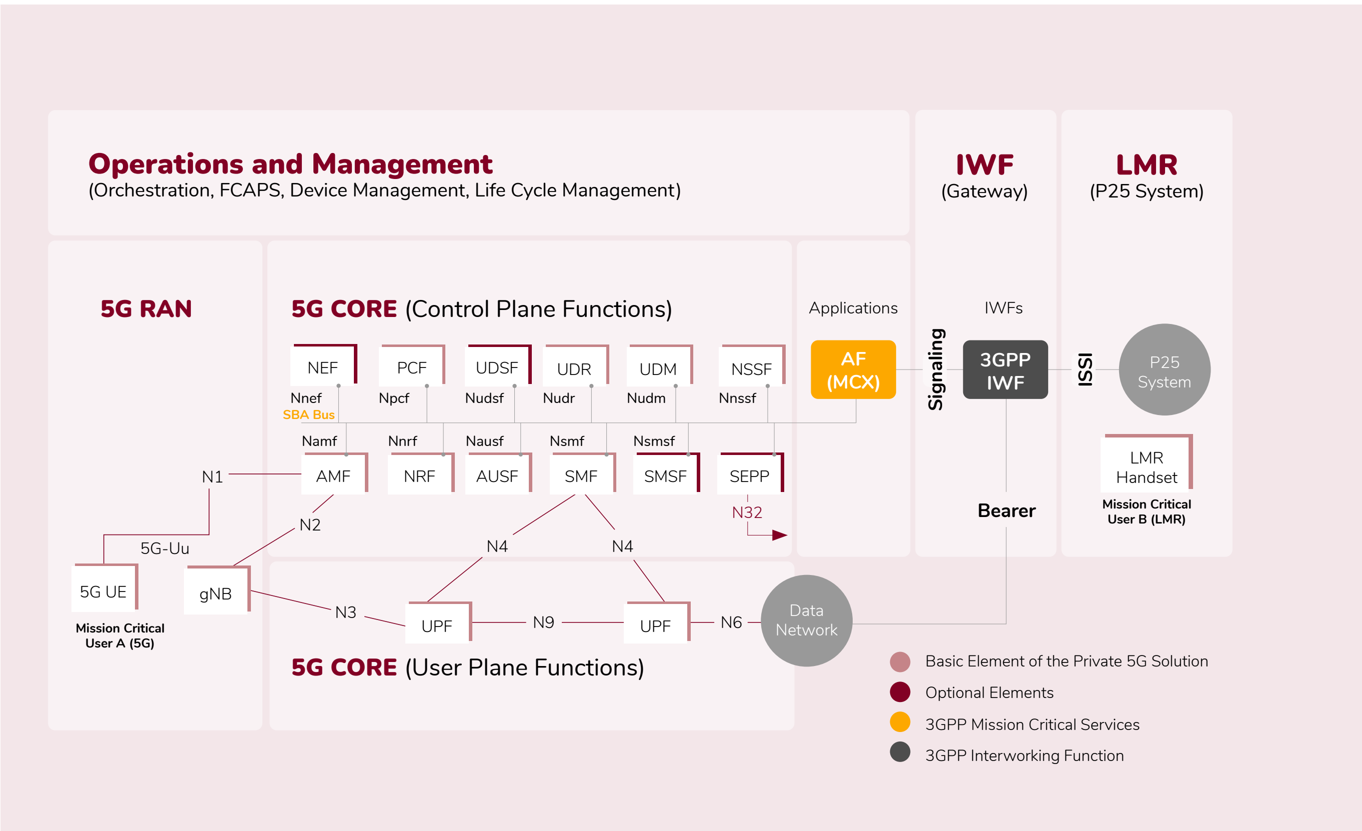
This integration is crucial in sectors requiring high mobility or remote access, such as aviation, maritime, and emergency services during large-scale disasters like earthquakes and tsunamis. It also supports expansive IoT deployments for autonomous vehicles, military communications, and urban infrastructure management. By ensuring continuous, reliable coverage for moving assets and remote installations, this synergy between 5G and satellite technology enhances operational efficiency and ensures high-quality service across both densely populated and isolated regions.

This synergy between LMR and 5G represents a forward-thinking approach that builds upon the strengths of existing infrastructure while embracing the possibilities of next-generation communications. The deployment of private 5G ensures a future-proof infrastructure that is adaptable, robust, and capable of supporting complex mission-critical operations, thereby transforming how agencies and industries respond to and manage critical situations. This paradigm shift not only enhances the effectiveness of emergency responses but also sets a new standard for future communications in a hyper-connected world. Moreover, when integrated with satellite technology, this advanced infrastructure extends even further, offering global reach and ensuring consistent connectivity in even the most remote or challenging environments. This combination maximizes the potential for technological innovation and reliability, fundamentally changing the landscape of global communication and response capabilities.

Understanding the 3GPP
Mission Critical System

This section explores the main components of the 3GPP mission-critical system. It outlines how the system adheres to the rigorous standardization protocols established by the 3rd Generation Partnership Project (3GPP), the entity responsible for evolving standards such as LTE, IMS, and now 5G along with mission-critical services. We also discuss the Interworking Function (IWF) specifications by 3GPP that ensure compatibility with traditional Land Mobile Radio (LMR) systems like P25, enhancing reliability and efficiency in mission-critical communications.

The key components of this system include the 5G Radio Access Network (5G RAN), the 5G Core, the 3GPP Mission Critical Applications (MCX) Server, and the 3GPP Interworking Function (IWF). Each component is vital for robust and efficient communication, delivering advanced capabilities and ensuring interoperability for modern public safety communications.



5G Radio Access Network (RAN)

The private 5G Radio Access Network (RAN), features the gNB base station for radio resource management, and provides robust wireless connectivity with high data rates, low latency, and broad coverage essential for mission-critical operations. The 5G RAN supports a wide range of frequency spectrums, including low-band, mid-band, and high-band frequencies.

Optionally, the gNB can be implemented using the O-RAN (Open Radio Access Network) architecture, which is structured into three distinct components: the Centralized Unit (CU), the Distributed Unit (DU), and the Radio Unit (RU). The CU is responsible for handling the control plane of the network, managing session control and mobility management, which are crucial for maintaining network integrity and user connections. The DU processes the user plane, handling data encoding, decoding, and forwarding, ensuring efficient data transmission across the network. The RU, closest to the end-users, focuses on the radio interface, converting digital signals into radio frequencies and vice versa, directly interfacing with user devices. This architecture offers significant advantages, such as the ability to implement multi-vendor platforms and the flexibility to strategically distribute these units across the network to meet specific operational requirements. This modular approach enhances overall network performance and adaptability.

5G Core Network

At the heart of the 3GPP Mission Critical network lies the 5G Core Network. The key elements that make up the core are the AMF (Access and Mobility Function) for managing user access and mobility; the SMF (Session Mobility Function) for session management; the UDM (Unified Data Management) for user data management; the AUSF (Authentication Server Function) for authentication of subscribers, the UDR (Unified Data Repository) for user data storage, the PCF (Policy Control Function) for policy control, the NRF (Network Repository Function) for maintaining an inventory of all network functions and their profiles, the NSSF (Network Slice Selection Function) for managing the network slices, and the UPF (User Plane Function) for forwarding of data, voice, and video traffic. This core network was designed for performance, reliability and operational efficiency thanks to the implementation of CUPS (Control User Plane Separation), SBA (Service Based Architecture), microservices and it's cloud native building blocks.

3GPP Mission Critical Applications (MCX) Server

In a Private 5G architecture, mission-critical services are supported by the implementation of the 3GPP MCX server, a crucial network function that delivers services like Mission Critical Push-to-Talk (MCPTT), Mission Critical Data (MCData), and Mission Critical Video (MCVideo). These applications, based on 3GPP specifications, follow the development path of 4G and 5G functionalities.

Mission-Critical Push-to-Talk (MCPTT):

MCPTT provides reliable and instantaneous voice communication for individual or group users in mission-critical situations. It includes features such as group and private calls, audio cut-in, and first-to-answer calls, with the capability to dynamically merge multiple groups or users in real-time, enhancing incident management and coordination among first responders.

1

Mission-Critical Video (MCVideo):

MCVideo provides real-time video streaming capabilities, allowing dispatchers to make informed decisions during emergencies. Features such as video-pull, video-push, and the ability to mark calls as “emergency” ensure high-priority access to visual information, improving situational awareness and response effectiveness.

2

Mission-Critical Data (MCData):

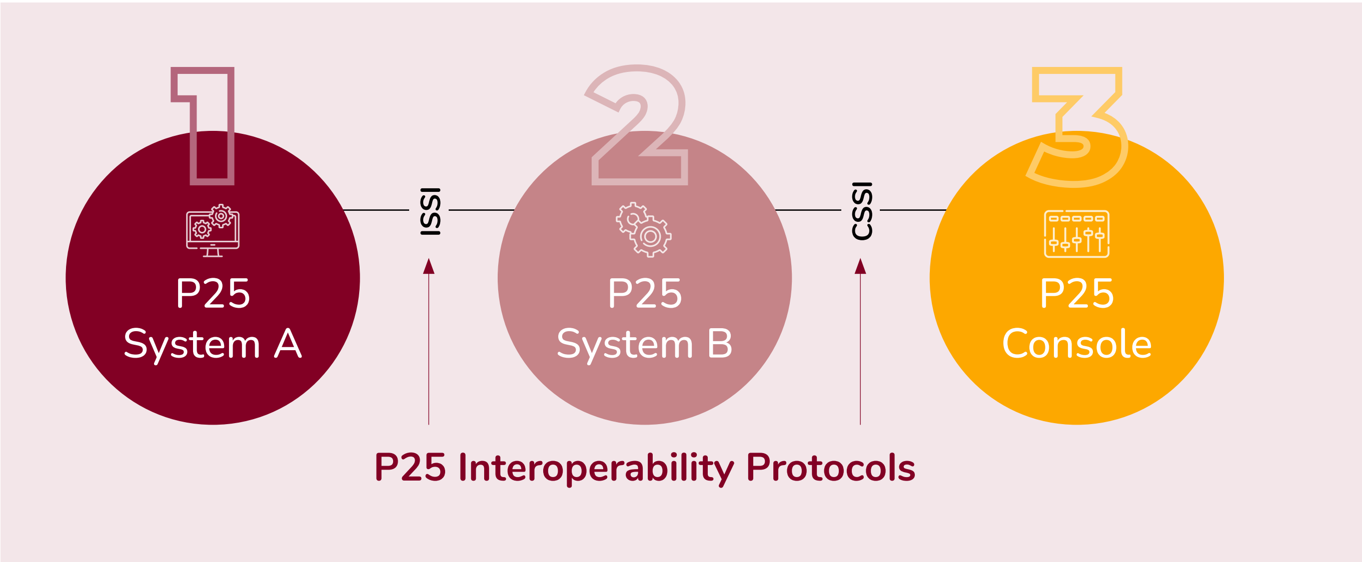
MCData supports the transmission and reception of critical information beyond traditional voice communication. It offers messaging, file distribution, and data streaming, enabling first responders to quickly share pictures, videos, and command messages with control rooms. This enhances situational awareness and aids in better decision-making during emergencies.

3

3GPP Interworking Function

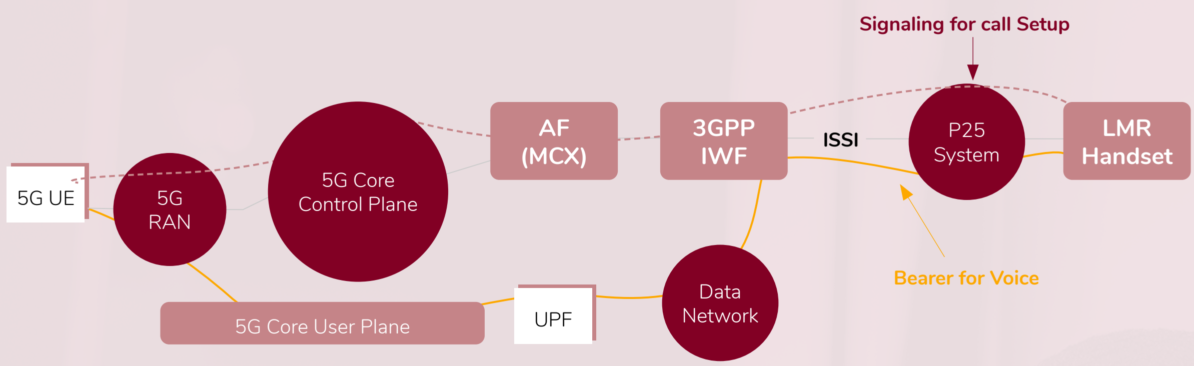
Public safety agencies nationwide use LMR systems like P25, which have been in operation for over two decades. As part of its evolution, P25 leverages the Inter-RF Sub-System Interface (ISSI) protocol to interoperate with other P25 systems over an IP transport, thus achieving multi-vendor interoperability, and extending geographical coverage.

As shown in the figure below, the Inter-RF Sub-System Interface (ISSI) enables a standardized means of interworking signaling messages among P25 LMR systems from different vendors. Interoperability with a 3rd party Dispatch Console system can be achieved with the implementation of the Console Sub-System Interface (CSSI), which enables a standardized means of interworking dispatch console signaling messages among different vendor products.



An existing P25 LMR system can integrate with a private 5G mission critical system via a gateway that supports the 3GPP IWF protocol per 3GPP TS 23.283. This gateway provides the interworking between the P25 LMR side (ISSI) and the 3GPP Mission Critical Sever (MCX). It should be noted that the gateway function does not necessarily represent a separate entity, and it may be already supported by the P25 LMR product vendor.

As illustrated in the figure below, the 3GPP IWF is involved in the setup of the call (control plane) and the voice bearer (user plane). Assuming a user on the P25 network establishes a voice call with a user in the private 5G network, the 3GPP IWF gateway translates the P25 signaling and media into a format compatible with 3GPP MCX services.



The process of integrating LMR/P25 technologies with 3GPP-based Mission Critical applications (MCX) will be gradual, taking a few years for evolution. In the meantime, legacy systems will coexist, making standards-based interoperability between LMR and MCX systems crucial for many public safety agencies. The implementation of standards-based interworking solutions simplifies the shift from legacy to modern technology and cuts down on costs. The specifications in 3GPP Release 16 completed the standardization of interworking with LMR systems, offering a framework for the basic functionalities needed for the interworking of MCPTT and MCData services with legacy LMR systems.

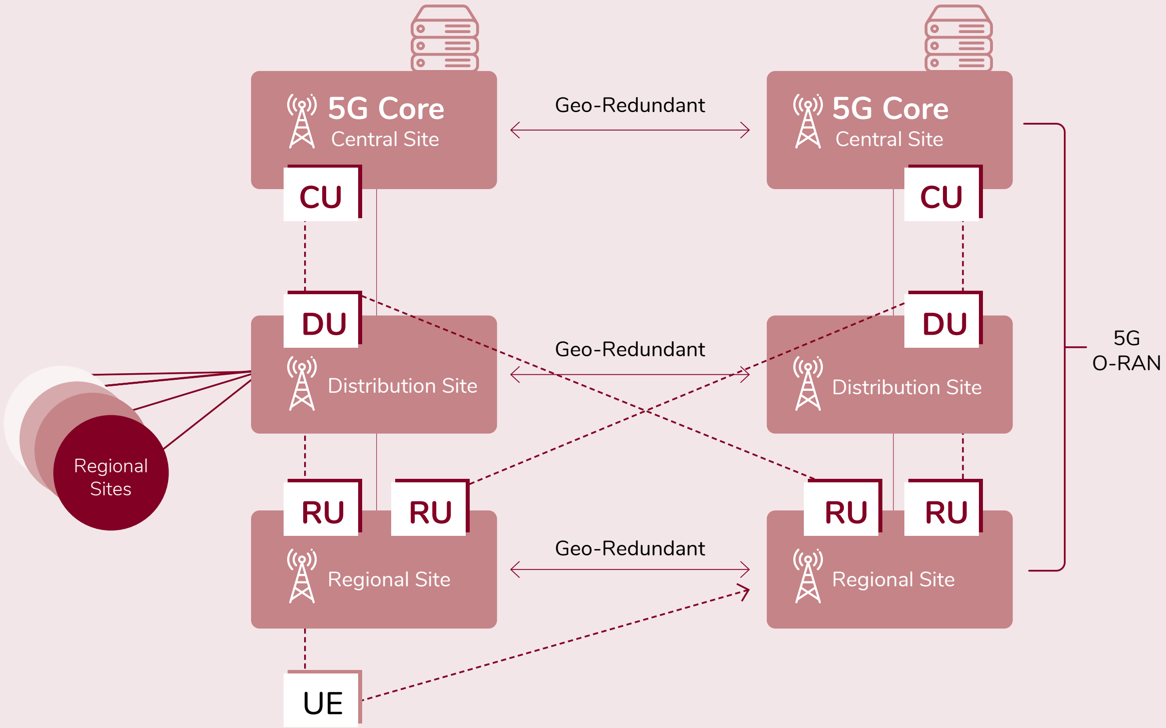
Designing 3GPP
Mission Critical Systems

The network design of a 3GPP mission critical system that leverages private 5G technology can be a complex task given the range of attributes and capabilities offered, including multi-site network design, redundancy, Quality of Service (QoS), security, edge computing, network slicing, and integration with existing LMR systems and complementary technologies such as satellite.

The design process must carefully consider the specific needs of the mission-critical use cases, which often require highly resilient, low-latency capabilities, particularly for those involving high definition on-demand real time video. In contrast, certain IoT applications may not demand low latency or high capacity. Therefore, it is important to thoroughly assess and understand the use cases, number of devices, data volume, and latency requirements to design the network effectively to meet these diverse needs. The following sections highlight some of the key considerations that make up an optimal network design for a mission critical network.

Multisite Network Design

Private 5G is based on a cloud-native architecture where several network functions that make up the 5G Core and the 5G RAN can be strategically distributed among central, distribution and regional sites. The number of sites will depend on the size of the Enterprise, the level of redundancy expected, and the geographic distribution of the users. It is important to understand the role of each network function and the latency requirements. In most deployments, the central sites handle network management tasks, orchestration tasks, and control plane network functions, while network functions that that deal with user plane traffic are placed at the regional sites closer to the users. For those latency-sensitive control plane functions, it may be best to place them either at regional sites or perhaps at a distribution site that sits between the central and regional sites. For example, a Radio Access Network based on O-RAN (Open-RAN) decomposes the gNB into three distinct elements; Central Unit (CU), Distributed Unit (DU), and Radio Unit (RU). The RU should be placed at the regional site to provide better access to the users, while the CU unit has more latency tolerance and can be placed at the central site. The DU unit on the other hand would benefit from being closer to the user by being either collocated at the regional site or being placed on a distribution site to aggregate several RUs placed at several regional sites.



Redundancy

To ensure resilience in mission-critical systems leveraging private 5G technology, network design must incorporate comprehensive redundancy at all levels. This includes redundant 5G core network components, control nodes, and critical hardware such as base stations, ensuring no single points of failure for all expected logical transmission paths. Geo-redundancy for central, distribution and regional sites involves having standby sites in different locations to handle traffic seamlessly in case of site failures. Each site should include a co-located redundant location in an active-active configuration, sharing traffic equally to ensure redundancy. Geo-redundancy between strategic sites is crucial for disaster recovery, with traffic balanced so each site operates at no more than 50% capacity to handle failures effectively.

Quality of Service (QoS)

In a Private 5G solution there are well defined Quality of Service (QoS) mechanisms with IP flow granularity available for prioritizing mission-critical traffic over less critical data. By assigning different priority levels to various types of data, the network ensures critical communication receives the necessary bandwidth and low latency, maintaining the integrity and performance of essential services. Network design should include detailed QoS policies that prioritize mission-critical traffic, specifying traffic classes and making proper mapping to the DSCP (Differentiated Services Code Point) markings that are used at the network level. It should also cover dynamic bandwidth allocation techniques to ensure availability during peak times or emergencies, and document congestion management strategies, including traffic shaping, policing, and queuing mechanisms, to prevent congestion from impacting critical services.

Security

A common misconception is that private 5G networks are more vulnerable to cyberattacks compared to traditional LMR systems. However, private 5G is equipped with advanced security features, including strong encryption protocols, secure key management, robust authentication mechanisms, and AI integration. A good network design should leverage these features, along with the proper security implementation for the cloud and networking environment and a zero-trust architecture to provide effective dynamic security policy enforcement and rapid threat response, making the network highly secure and adaptable to emerging threats. By leveraging these advanced security measures, the network is protected from sophisticated cyber threats, ensuring data confidentiality and network integrity.

Network Slicing

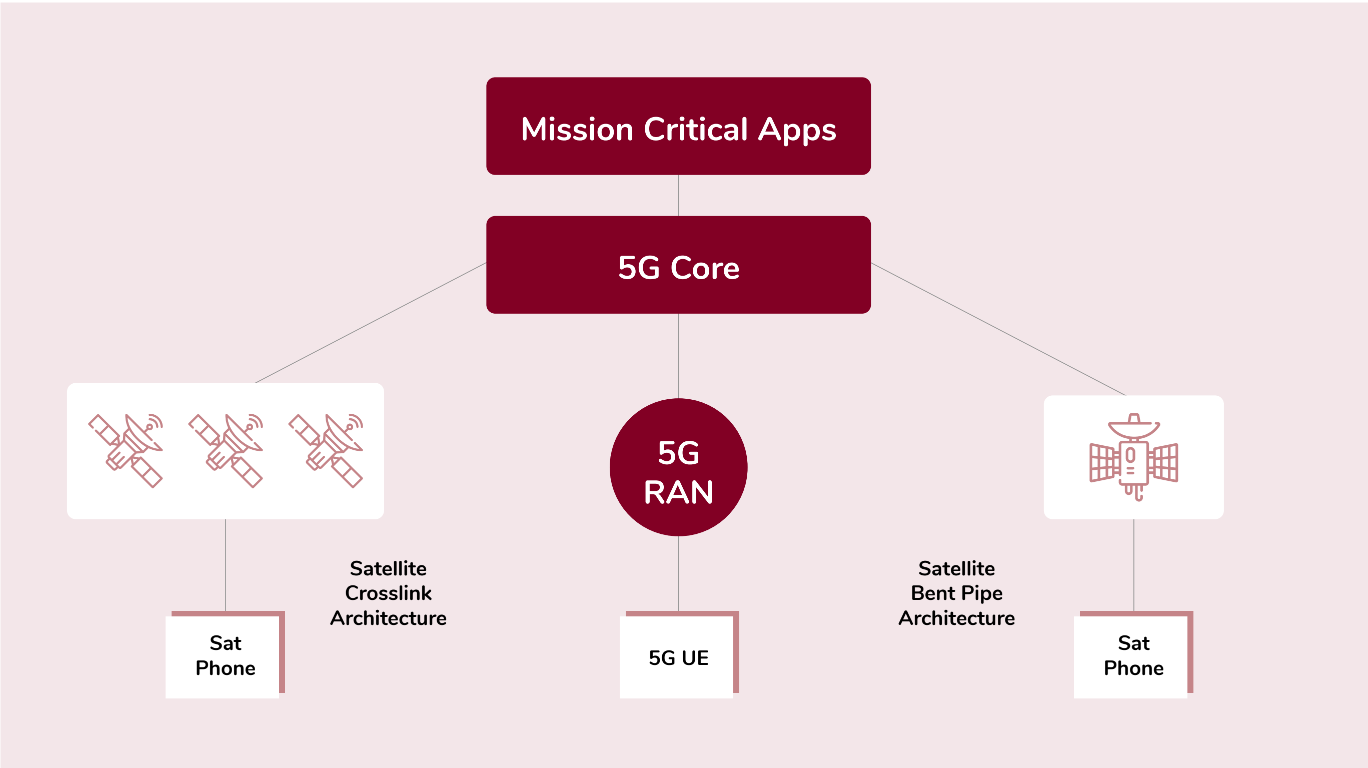
Network slicing is a network architecture concept that allows multiple virtual networks to be created on top of a shared physical infrastructure. In the context of network design for mission-critical systems, careful examination of the requirements will determine if network slicing is needed. For example, if the private 5G network is shared among several agencies, it would be beneficial to dedicate multiple network slices to isolate and allocate resources based on the needs of specific applications, services, or agencies. Each slice can be designed to meet the unique performance, security, and reliability requirements of different mission-critical services, ensuring that each application operates optimally without interference from others.

Edge Computing

Edge computing is a distributed computing paradigm offered by 5G that brings computation and data storage closer to the location where it is needed, to improve response times and save bandwidth. Instead of processing data in a centralized data center or cloud, edge computing processes data on local devices or edge servers located near the data source. Deploying edge computing capabilities ensures that mission critical functions can continue to operate without dependency on network resources deployed at central sites. Furthermore, processing data closer to the source reduces latency and bandwidth usage, improving the responsiveness and reliability of mission-critical applications.

Non-Terrestrial-Network (NTN)

Some mission critical environments may require the services of a Non-Terrestrial-Network to increase coverage. The network design needs to consider the different network satellite architectures available to meet the needs of the use cases. In particular, the latency should be evaluated to provide an optimal design. For example, when leveraging Low Earth Orbit (LEO) satellite system, there are a few architectures that can be implemented. As illustrated in the figure below, some satellite providers use Bent Pipe architecture, while others may use Crosslink. If the traffic is very sensitive to latency, the Bent Pipe approach may be a better option given that latency between the satellite phone and the terrestrial phone would be lower due to a single satellite hop.



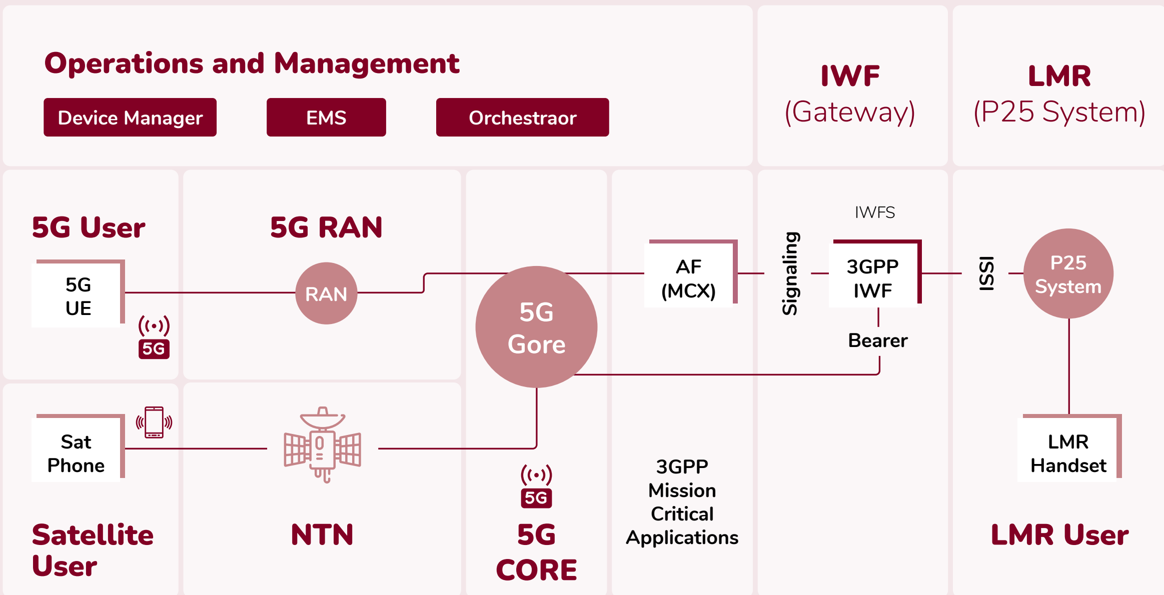
Implementing 3GPP Mission Critical Systems

An effective implementation and integration strategy is crucial when merging legacy Land Mobile Radio (LMR) systems with a modern 3GPP-based mission-critical system that leverages private 5G technology. Public safety agencies, which rely heavily on their existing LMR infrastructure for mission-critical communications, must ensure seamless interoperability between systems. This integration with a private 5G system should occur in a gradual, phased manner to minimize disruptions, considering the varied nature of existing deployments and the need for extensive interoperability testing. The new 3GPP/5G system will operate alongside the existing LMR/P25 systems, including rigorous testing for voice and feature interoperability to maintain continuous accessibility of mission-critical services.

Lab Environment for Interoperability and Functionality Testing

Creating a lab environment is the initial step in the integration process, where extensive interoperability tests are conducted under controlled conditions that mimic real-world scenarios. This testing phase is crucial for assessing how the new 3GPP/Private 5G mission-critical system interacts not only with the existing LMR system, ensuring comprehensive fulfillment of all use cases and feature interaction. The lab environment will facilitate network simulations that address 5G-specific challenges such as increased data rates, lower latency, and higher mobility, critical for testing the network's ability to handle diverse operational demands.

Moreover, the interoperability testing will also focus on validating the performance of mission-critical push-to-talk (MCPTT), video, and data services over 5G, while assessing compatibility with existing P25 systems. It is essential to include tests that verify the private 5G environment's interoperability with satellite networks to ensure appropriate Quality of Service (QoS) results for each of the required use cases. The Acceptance Test Plan developed during this phase will outline specific tests and criteria needed to confirm that the integrated systems meet the necessary performance and reliability standards, thereby guaranteeing a seamless and effective deployment of the new mission-critical network infrastructure.

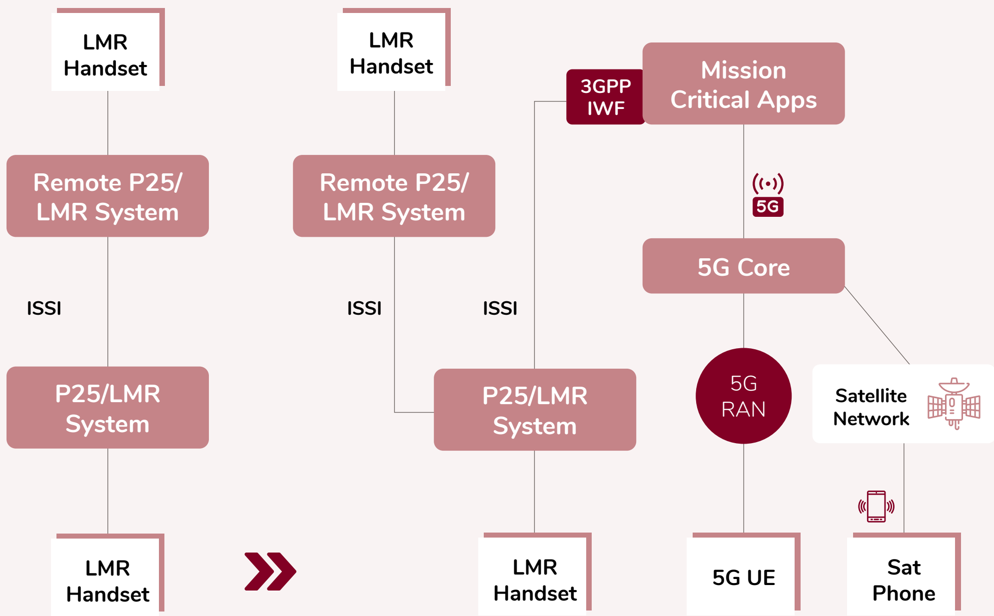


Lab Environment for Interoperability and Feature Testing

Phase 2

Deployment of a Converged System

After successful lab validation, field implementation begins, focusing on the integration and convergence of the existing P25/LMR with the new 3GPP/5G mission-critical system. For some environments, integration of the 5G core to satellite based access will be part of the plan to extend coverage beyond 5G RAN reach. This phase starts with a detailed coverage and capacity analysis of the existing P25 network to identify where mission critical enhancements are necessary, particularly in urban areas with dense user populations and high data demand. The design of a hybrid network will incorporate not only the core network components and RAN elements but also advanced 5G capabilities such as network slicing for prioritized mission-critical communications and edge computing to reduce latency for critical applications. This holistic approach ensures that both networks complement each other, maximizing the benefits of high reliability and enhanced data capabilities.



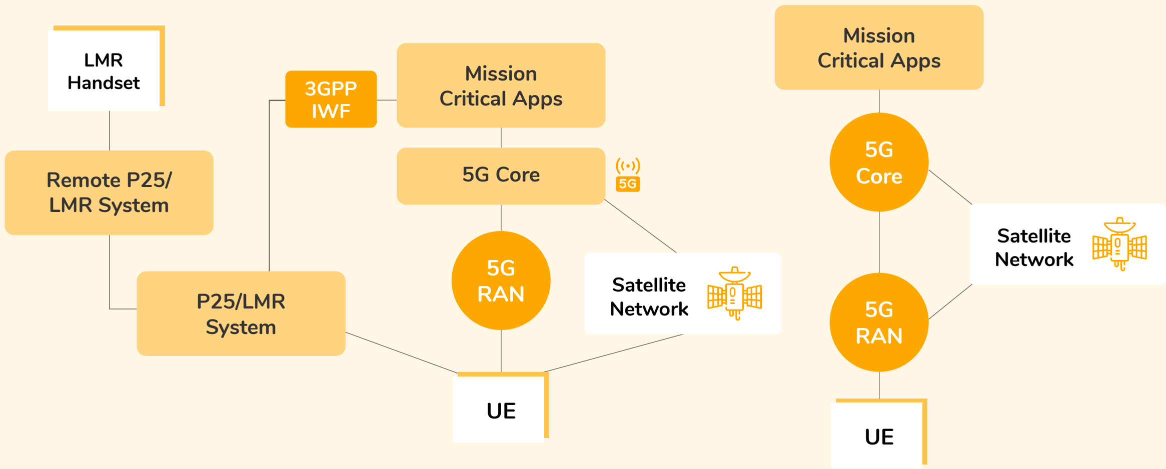
Mission Critical Deployment Today

Mission Critical Converged Deployment

Phase 3

Deployment of Multi-Access Handsets

With the operational readiness of the new system, transitioning to multi-access handsets that support P25, 3GPP/5G and Satellite networks becomes crucial. This phase includes rigorous lab testing of multi-access handover operations and expected feature capability to ensure these handsets can seamlessly switch between networks without service interruptions and get access to the expected features. Field deployment of these handsets follows, with comprehensive training for end-users to optimize their use of the new technology.



Mission Critical Converged Deployment With multi-access Handsets

Mission Critical Private 5G Deployment

Throughout this process, collaboration with experienced system integrators and technology vendors skilled in both LMR and private 5G technologies will be indispensable. These partnerships will facilitate robust and effective integration, handling complex network configurations and ensuring a smooth transition to a technologically advanced mission-critical communication system.

Requirement for Successful Integration

The successful integration of Land Mobile Radio (LMR) systems with 5G technology for mission-critical applications requires a unique blend of expertise that spans both traditional public safety communications and cutting-edge network technologies. This necessity for specialized integrators stems from the complex nature of the transition and the critical importance of maintaining seamless, reliable communications for public safety agencies.

Here's why an experienced integrator is crucial:

01

Optimizing Network Design for Public Safety Needs:

5G network architecture, while powerful, needs to be tailored specifically for public safety applications. An integrator with experience in both fields can design a network that meets the unique requirements of emergency services, including coverage in challenging environments, prioritization of critical traffic, and support for specialized applications.

02

Navigating Complex Interoperability Challenges:

The integration of LMR and 5G involves intricate interoperability issues. An experienced integrator can navigate these challenges, ensuring that legacy LMR systems can communicate effectively with new 5G networks. This includes understanding protocols like P25, TETRA, and 3GPP standards, and how they can be bridged to create a seamless communication ecosystem.

03

Deep Understanding of Both Worlds:

An integrator with experience in both LMR and 5G brings a comprehensive understanding of the strengths, limitations, and operational requirements of each technology. This dual expertise is essential for creating a cohesive system that leverages the best aspects of both LMR and 5G without compromising the reliability that mission-critical operations demand.

04

Ensuring Continuity of Critical Services:

Mission-critical communications cannot afford downtime or degradation during the transition. An integrator with a background in public safety LMR understands the non-negotiable need for constant availability and can design integration strategies that maintain uninterrupted service throughout the migration process.

05
Managing the Gradual Transition:

The shift from LMR to 5G is not an overnight process. It requires careful planning and execution over an extended period. An experienced integrator can develop and implement a phased approach that allows agencies to gradually adopt new technologies while maintaining existing operations.

06
Addressing Security and Reliability Concerns:

Public safety communications demand the highest levels of security and reliability. An integrator versed in both LMR and 5G can implement robust security measures that protect sensitive communications across both legacy and new systems, ensuring that the integrated network meets or exceeds the stringent requirements of public safety agencies.

07
Leveraging Advanced Features While Maintaining Simplicity:

5G offers advanced features like high-bandwidth data transmission and low latency communications. However, these must be integrated in a way that doesn't overwhelm users accustomed to simpler LMR systems. An experienced integrator can balance the introduction of new capabilities with the need for intuitive, reliable operation under stress.

08
Cost-Effective Implementation:

With expertise in both technologies, a skilled integrator can design solutions that maximize the use of existing infrastructure while strategically introducing new elements. This approach can significantly reduce costs and provide a better return on investment for public safety agencies.

09
Regulatory Compliance and Spectrum Management:

The regulatory landscape for public safety communications is complex and varies by region. An integrator with experience in both LMR and 5G will be well-versed in navigating these regulations, ensuring compliance while optimizing spectrum usage across both technologies.

10
Future-Proofing the Network:

As technology continues to evolve, the integrated network must be designed with future expansion and upgrades in mind. An experienced integrator can create a flexible architecture that accommodates emerging technologies and changing operational needs.

Conclusion

The integration of Land Mobile Radio (LMR) systems with 3GPP-based mission-critical applications leveraging private 5G technology represents a significant advancement in public safety communications. Key benefits of this integration include improved scalability and availability through cloud-native architecture, enhanced bandwidth capacity for advanced data services, wider spectrum utilization, better vendor interoperability, AI integration for network optimization and security, and extended coverage through Non-Terrestrial Networks. The 3GPP mission-critical system, comprising the 5G RAN, 5G Core, MCX Server, and Interworking Function, provides a standardized framework for seamless integration with existing LMR systems.

The design and implementation of such integrated systems require careful consideration of multisite network architecture, redundancy, Quality of Service, security measures, network slicing, and edge computing capabilities. A phased approach to implementation is recommended, starting with lab testing, followed by converged system deployment, and finally the introduction of multi-access handsets.

Crucially, the success of this integration hinges on the expertise of system integrators experienced in both LMR and 5G technologies. These specialists play a vital role in navigating complex interoperability challenges, ensuring continuity of critical services, and optimizing the network design for public safety needs.

As public safety agencies look to modernize their communication infrastructure, the integration of LMR with 3GPP mission-critical systems over private 5G networks offers a future-proof solution. This approach not only enhances current capabilities but also paves the way for ongoing technological advancements in mission-critical communications, ultimately improving the effectiveness and efficiency of emergency response operations.

About Commdex

For over 20 years, Commdex has been providing a broad, rich portfolio of proven network solutions to Government and Enterprise customers for the deployment of telecom networks, facilities, and supporting systems. Commdex specializes in designing and implementing mission-critical voice and data networks over 5G, microwave, land mobile radio, DAS, SATCOM, and other technologies. Its solutions, services, and methodologies have been tested and proven in hundreds of customer environments nationwide. With its ability to design 5G Solutions coverage and our experience in regional and statewide systems, Commdex has not only the technical expertise to build the systems but also the management expertise to aid in the integration and operation.

Based on its years of experience in implementing large, complex systems, Commdex has perfected an integrated approach that maximizes the capability of any solution that a customer may require while minimizing the associated risks, schedule, and cost. This iComm360o approach ensures that the project is delivered with proven expertise through the capability of a proven integrator that understands the entire life cycle of Communications projects. This experience gives it the ability to confidently and quickly implement the 5G network.

For more information

CLICK HERE