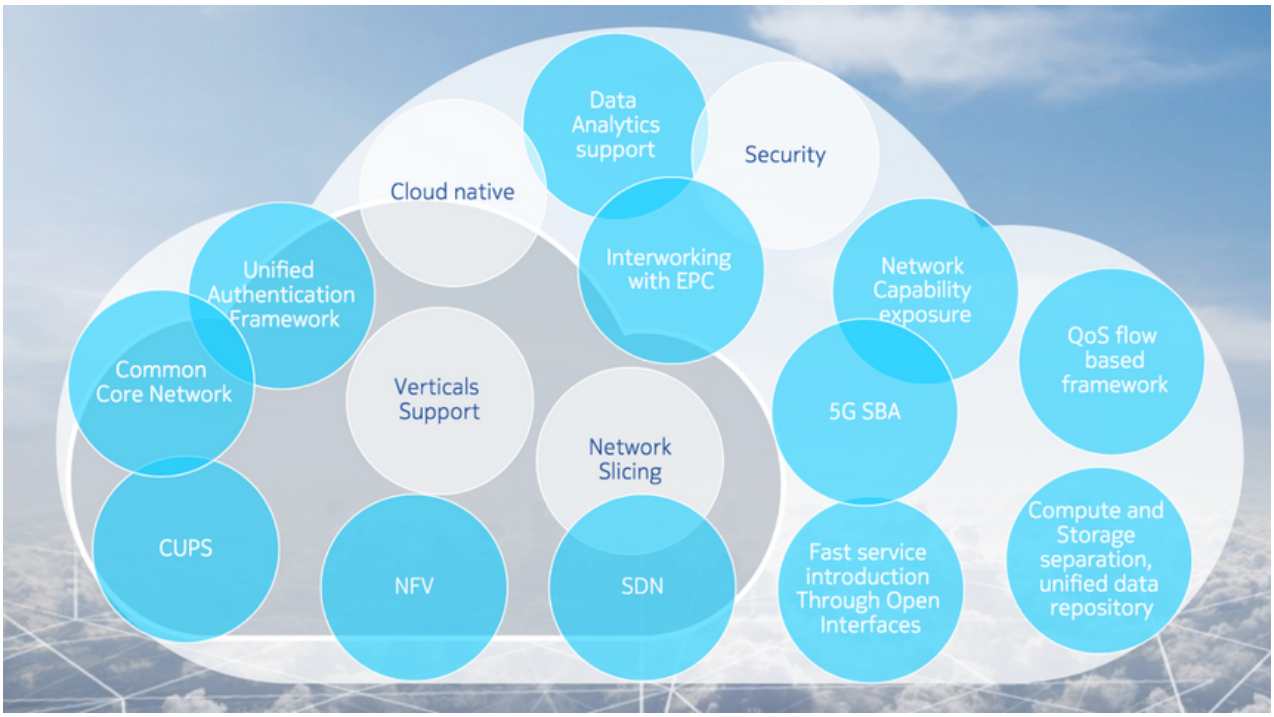
COMMDEX

5G ARCHITECTURE FOR MISSION CRITICAL COMMUNICATIONS

INTRODUCTION

5G technology is the next generation of wireless technology that promises to revolutionize the way we communicate and connect with each other. It is a step forward in the evolution of mobile networks, bringing faster speeds, increased capacity, and lower latency to enable more innovative and efficient services. One of the most promising areas of application for 5G is public safety, where it can help improve emergency response times, enhance situational awareness, and support the coordination of first responders. In this whitepaper, we will provide an overview of 5G architecture for public safety and highlight its key features and benefits.



5G Capabilities

BENEFITS OF 5G TECHNOLOGY
FOR PUBLIC SAFETY

The use of 5G technology in public safety has several benefits, including:

High network speed
For public safety agencies, higher network speeds will make it possible to send large amounts of data (such as high-definition video) over the wireless network in real time.

Low latency
Latency is the time it takes a network to respond to a request. 5G promises to cut latency down to 1-2 milliseconds allowing critical life-or-death operations via remote connection.

Improved situational awareness
5G networks provide real-time information about the location, status, and needs of first responders, allowing for more effective coordination and response.

Enhanced communication
5G networks offer faster speeds, higher capacity, and lower latency, which can improve the quality and reliability of voice and video communication between first responders.

More efficient resource allocation
5G networks can support the deployment of advanced analytics and machine learning algorithms that can help first responders make better decisions about resource allocation and deployment.

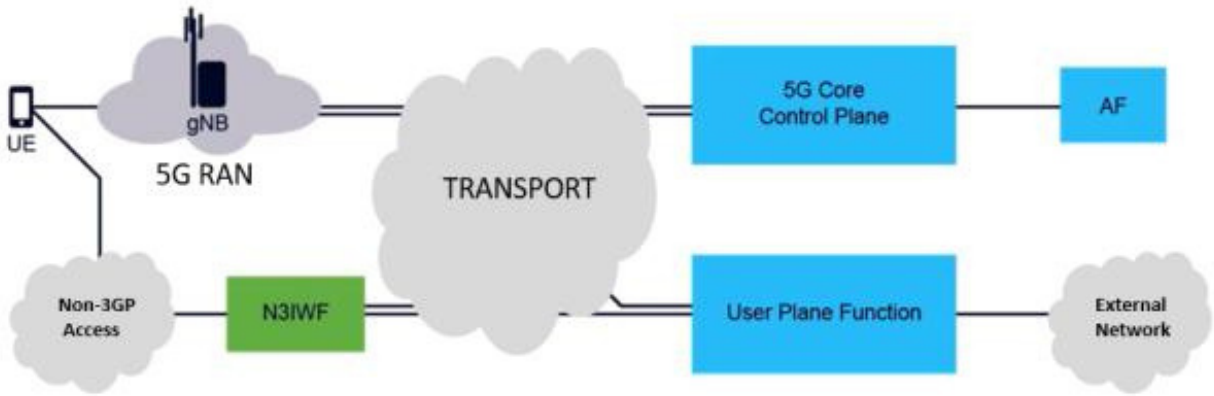
Increased safety
5G networks can support the use of advanced sensors and IoT devices that can monitor environmental conditions, detect hazardous materials, and alert first responders to potential dangers.

Interoperability
5G architecture for public safety communications has been designed to be interoperable with existing networks and systems, allowing for seamless integration and collaboration between different agencies and organizations.

Robustness
5G networks have been designed to be highly resilient and robust, with redundant components and failover mechanisms that can ensure the network remains operational even in the event of a failure or outage.

5G ARCHITECTURE
FOR PUBLIC SAFETY

The architecture of 5G networks for public safety is based on a set of standards and specifications that have been developed by the 3rd Generation Partnership Project (3GPP). These standards define the various components and interfaces of the network, as well as the protocols and procedures that govern their interaction. The 5G architecture for public safety is designed to be flexible and scalable, able to adapt to different types of emergencies and situations. As illustrated in the figure below, an end-to-end 5G private network is composed of the UE (User Equipment), the 5G RAN (Radio Access Network), the 5G Core, the transport, access to an AF (Application Function) and connectivity to non-3GPP access networks and external networks. In order to enable the full potential of 5G capabilities, careful network design considerations must be implemented across all these network domains



Designing a private 5G network requires careful consideration of several key factors, including:

Coverage

A private 5G network must provide adequate coverage to meet the mobility and access needs of the intended users. This may involve conducting a site survey to identify potential coverage limitations and developing a deployment plan that includes the necessary infrastructure to provide coverage throughout the intended area.

Capacity:

The network must have sufficient capacity to support the number of devices and applications that will be connected to it. The transport network must be carefully assessed and traffic engineered to meet the routing and latency requirements of control and data plane user traffic in the upstream and downstream direction. This requires consideration of the expected traffic volume, the types of applications being used, and the number of users accessing the network simultaneously.

Security

As a private network, security is a paramount concern. The network should be designed with strong authentication and encryption protocols to protect against unauthorized access and data breaches. Implementation of firewall functions at the peering points to external networks and proper configuration and enforcement of network access policies is important.

Interoperability

The private 5G network should be designed to support interoperability with existing networks and devices, such as Wi-Fi and cellular networks, to ensure seamless connectivity for users. For non-3GPP access networks such as Wi-Fi, 5G implements an entity called N3IWF (N3 Interworking Function), which allows interoperability with the 5G Core.

Quality of Service (QoS)

Different applications may require different levels of QoS, such as low latency or high bandwidth. The private network should be designed to support these varying requirements and ensure that the network is optimized to deliver the necessary QoS. It is imperative that the network QoS design considers the Layer 2 and Layer 3 transport aspects to ensure proper priority is given to the 5G control, user plane and management 5G traffic.

Management and maintenance

A private 5G network requires ongoing management and maintenance to ensure optimal performance and reliability. This may involve developing a management plan that includes regular maintenance, monitoring, and troubleshooting procedures.

Regulatory compliance

Depending on the location and intended use of the private network, it may be subject to regulatory compliance requirements, such as obtaining necessary licenses or adhering to specific technical standards. These requirements should be carefully considered and incorporated into the network design.

The key components of 5G architecture for public safety include:

Radio Access Network (RAN)

The RAN consists of a set of base stations that provide wireless coverage to the UE. These base stations are connected to the core network via high-speed fiber optic links. The RAN is responsible for connecting devices to the 5G network and transmitting data wirelessly over the air interface. It includes a set of base stations or access points, antennas, and other supporting infrastructure, such as backhaul connections.

Core Network (CN)

The CN is the backbone of the 5G network and is responsible for managing the UE, the RAN, and the various applications and services that are used by first responders. The CN is made up of several components, including the User Plane Function (UPF), the Session Management Function (SMF), the Authentication Server Function (AUSF), and the Network Exposure Function (NEF).

The core network provides the intelligence and processing power for the 5G network. It includes components concepts such as the mobile multi-access edge computing (MEC) platforms, software-defined networking (SDN) controllers, and network functions virtualization (NFV) infrastructure.

Security

Security is a critical aspect of 5G architecture for public safety, as it is essential to ensure the confidentiality, integrity, and availability of the network and the data that is transmitted over it. 5G networks use a variety of security mechanisms, including encryption, authentication, and access control, to detect and protect against threats and attacks at different layers of the protocol stack for user plane and control traffic.

User Equipment (UE)

The UE refers to the devices that are used by first responders, such as smartphones, tablets, and laptops. These devices are equipped with 5G radio modules and are able to communicate with the network. The devices that connect to the private 5G network can include a wide range of equipment such as smartphones, tablets, laptops, IoT devices, and industrial equipment. These devices must be compatible with the 5G network technology and support the necessary features and protocols.

Management and orchestration

The private 5G network requires management and orchestration tools to monitor network performance, automate network functions, and enable efficient resource allocation. These tools may include network management systems (NMS), Service orchestration platforms, and analytics tools.

Application Servers (AS)

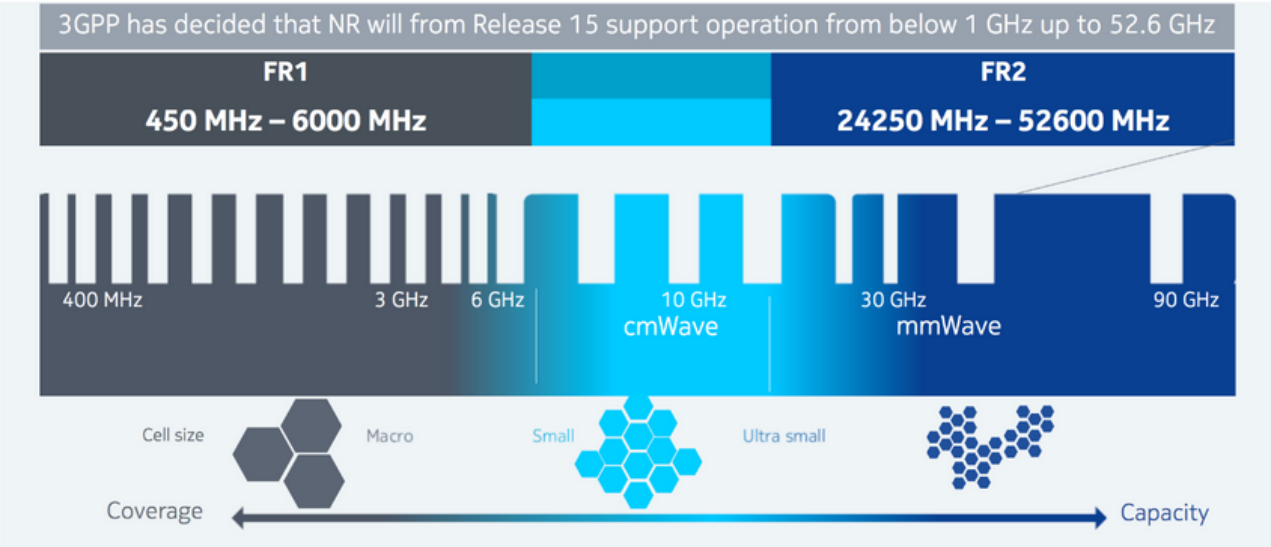
The AS provides the various applications and services that are used by first responders, such as voice and video communication, real-time location tracking, and sensor data analytics.

CAPACITY CONSIDERATIONS FOR 5G

Designing a 5G network requires careful consideration of several capacity-related factors, including:

Frequency bands

5G can operate in a range of frequency bands, including low, mid, and high bands. Each band has its own benefits and limitations in terms of coverage area and capacity. Low bands provide wider coverage, but have lower capacity. High bands, on the other hand, offer higher capacity but have limited coverage range. The figure below illustrates the frequency ranges supported by 5G



5G Spectrum Range

Antenna density

5G networks require more antennas than previous generations of mobile networks. This is because 5G uses a technology called beamforming, which uses multiple antennas to focus the signal in a specific direction. The number and density of antennas need to be carefully planned to ensure optimal coverage and capacity.

Backhaul

5G networks require high-capacity backhaul connections to transfer large amounts of data between base stations and the core network. The backhaul infrastructure needs to be designed to handle the increased capacity demands of 5G.

Core network capacity

The core network is responsible for processing and routing data between different parts of the network.

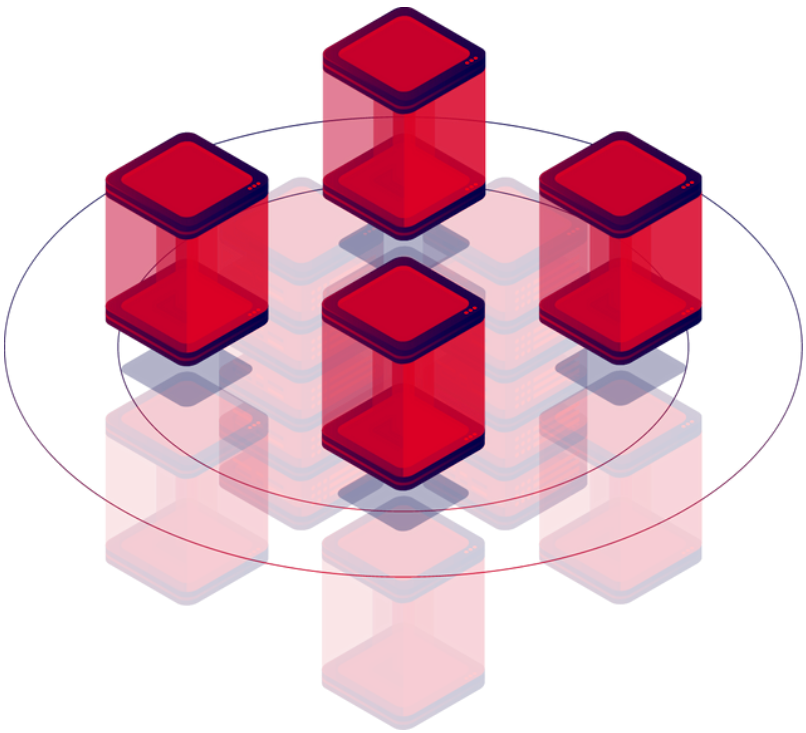
5G networks require a high-capacity core network to handle the increased traffic and data processing requirements

Network slicing

5G networks support network slicing, which allows operators to create multiple virtual networks on a single physical network infrastructure. Each network slice can have its own capacity and performance characteristics, allowing operators to optimize the network for different use cases and applications.

Traffic management

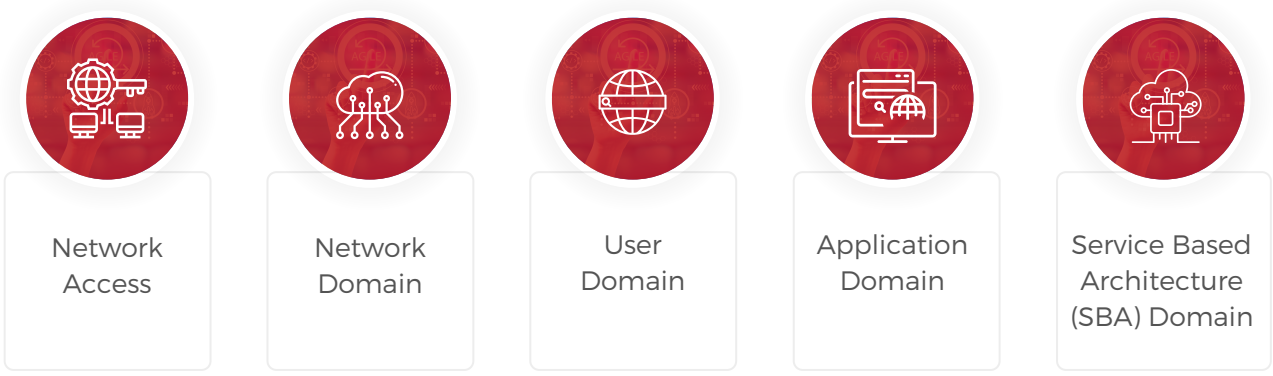
5G networks require advanced traffic management techniques to prioritize traffic and ensure that critical applications and services receive the necessary capacity and performance. This requires sophisticated traffic shaping and QoS mechanisms to manage the traffic flow across the network.



SECURITY CONSIDERATIONS FOR 5G

The security of 5G networks for mission-critical communications is of paramount importance. As 5G networks will be used for a wide range of public safety applications, including emergency response, disaster management, and law enforcement, it is essential to ensure that these networks are secure and resilient.

The 5G architecture has network functions that provide authentication, authorization, encryption, privacy, and integrity protection. All of these fall under one or more of the following security domains:

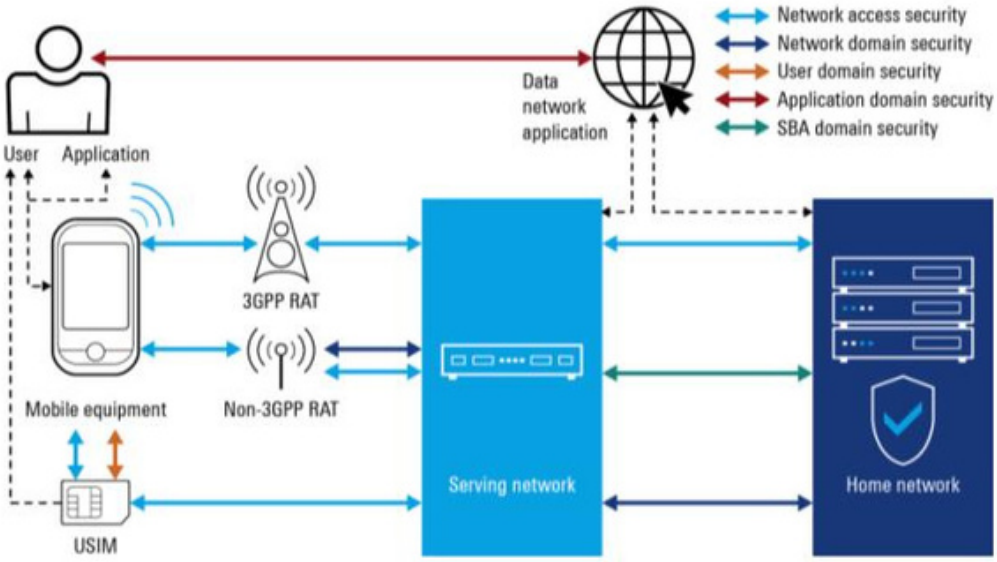


If we take for example, the 5G security feature in which the users's identity is never transmitted in clear text (is encrypted), this capability is addressing a security aspect of the user domain, the network access and the application domain.

If we take for instance, the role of the SEPP (Security Edge Protection proxy), which is part of the 5G Service Based Architecture and handles all communication between the home and visited networks to protect against DOS attacks, perform topology hiding and protect from unathorized usage, we have a network function that is addressing security aspects of the network domain and SBA domain.

A security capability of 5G that fits within the Network access domain category, is the concept of mutual verification. That is, the network verifies the UE is who he claims to be, but the UE also verifies the network as well. Several authentication options are available.

The figure below illustrates a high level view of the security domains associated with a 5G private Network. In order to meet the high standards of public safety networks, it is crucial to look at all possible security options available, select the appropriate ones, and implement an optimal security design that span all domains.



In this section, we will discuss key end-to-end design security measures that can be used to secure the 5G networks for mission-critical communications across all domains.

Encryption

Encryption is an essential security measure that can be used to protect the confidentiality and integrity of data transmitted over 5G networks. Encryption can be implemented at multiple layers of the network, including the user equipment, radio access network, and core network. The use of encryption can prevent unauthorized access to sensitive data, even if it is intercepted during transmission.

Authentication

Authentication is another important security measure that can be used to verify the identity of users and devices on the network. Strong authentication mechanisms can prevent unauthorized access and protect against attacks such as man-in-the-middle attacks and identity theft. Authentication can be implemented using a range of technologies, including digital certificates, biometrics, and two-factor authentication. The 5G architecture supports the concept of mutual verification. That is, the network verifies the UE is who he claims to be, but the UE also verifies the network as well. This happens over the NAS protocol for both 3GPP and non-3GPP network access types. The 5G architecture also allows the use of certificates, SIM based 5G-AKA or EAP-AKA authentication.

Access control

Access control is another key security measure that can be used to restrict access to sensitive resources on the network. Access control can be implemented at multiple levels of the network, including the user equipment, radio access network, and core network. By limiting access to sensitive resources, access control can prevent unauthorized access and protect against attacks such as denial-of-service attacks and network intrusions.

Network segmentation

Network segmentation is a security measure that can be used to partition the network into smaller, more manageable segments. By segmenting the network, it is possible to isolate sensitive resources and limit the impact of attacks. Network segmentation can also help to reduce the risk of lateral movement, where attackers move laterally through the network in search of sensitive resources.

Threat detection and response

Threat detection and response is a critical security measure that can be used to identify and respond to security incidents in real-time. By using a range of threat detection technologies, including intrusion detection systems, security information and event management (SIEM) systems, and security analytics, it is possible to detect and respond to security incidents quickly and effectively.

Physical security

Physical security is an often-overlooked security measure that is essential for securing 5G networks for mission-critical communications. Physical security measures can include secure facilities, access control systems, video surveillance systems, and security personnel. By implementing physical security measures, it is possible to prevent unauthorized access to critical resources and protect against physical attacks and tampering.

Redundancy and resiliency

Redundancy and resiliency are important security measures that can be used to ensure the availability and reliability of mission-critical communications. By implementing redundant systems and failover mechanisms, it is possible to ensure that critical resources remain available even in the event of a failure or outage.

CORE NETWORK

Designing a 5G core network requires careful consideration of several key factors, including

Cloud-native architecture

5G core networks are designed to be cloud-native, meaning they use cloud-based technologies to enable scalability, flexibility, and automation. This allows operators to deploy and manage the network more efficiently, reducing costs and increasing agility.

Service-based architecture

The 5G core network is based on a service-oriented architecture (SOA), which means that network functions are modular and can be deployed independently of each other. It also means that the network functions need to be authorized first to get services from other network functions. This allows operators to introduce new services and features more quickly and efficiently.

Network slicing

5G core networks support network slicing, which allows operators to create multiple virtual networks on a single physical network infrastructure. Each network slice can have its own capacity and performance characteristics, allowing operators to optimize the network for different use cases and applications.

Edge computing

5G core networks support edge computing, which allows processing and storage to be moved closer to the end user. This can reduce latency and improve performance for latency-sensitive applications, such as virtual and augmented reality.

Quality of service (QoS)

5G core networks need to support different levels of QoS to ensure that critical applications and services receive the necessary performance and capacity. This requires sophisticated traffic shaping and QoS mechanisms to manage the traffic flow across the network.

Integration with legacy networks

5G core networks need to be designed to integrate with existing 4G and 3G networks, as well as other legacy networks, to ensure a smooth transition to the new technology.

CONCLUSION

5G technology has the potential to transform the way public safety organizations operate, enabling more efficient and effective emergency response and coordination. The architecture of 5G networks for public safety is designed to be flexible, scalable, and secure, and offers several benefits over traditional mobile networks. As 5G technology continues to evolve, it is expected to play an increasingly important role in public safety, helping to save.

Securing 5G networks for mission-critical communications is a complex and challenging task. However, by implementing a range of security measures, including encryption, authentication, access control, network segmentation, threat detection and response, physical security, and redundancy and resiliency, it is possible to build a secure and resilient 5G network that can support a wide range of public safety applications. As the use of 5G networks for public safety continues to grow, it is essential to prioritize security and ensure that these networks are built with security in mind from the ground up.

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 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 iComm360™ 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, visit us at commdex.com.