MISSION CRITICAL APPLICATIONS OVER OPERATOR'S BROADBAND NETWORK WHITE PAPER

Executive summary

Critical communications can be categorized as Mission Critical and Business Critical or both. Public Safety organizations such as police, fire and rescue services collectively termed as Public Protection and Disaster Relief (PPDR), are referred to as Mission Critical users. Business Critical users, refer to users in Public Utilities, Oil & Gas, Transportation, etc. Critical communications are also essential to many more sectors.

The key drivers for critical communications are safety, security and operational efficiency. Ultimately, these drivers directly translate to economic value for these sectors.

Critical communication services have been built on dedicated networks and spectrum, with specialized communication technologies such as TETRA, DMR and P25, collectively referred as Private Mobile Radio (PMR), being the mainstream digital communication technologies. Service operators for these specialized communication technologies are typically government controlled, with serving only mission critical users their priority. The Push-to-Talk (PTT) functionality, a characteristic of critical communications enabling one-to-many group communication with a simple button-triggered action, combined with command and dispatching applications have enabled a high level of efficiency in daily operations and emergencies. These functions have also become desirable for business critical users.

> On the other hand, *TETRA, DMR and P25 are narrowband technologies capable of only voice services and limited short data services, unable to equip critical communication users with capabilities for broadband applications much needed today. Demand for data applications such as push-to-video, real-time video surveillance and location-based services is pushing critical communications to adopt new technologies.*

Technology evolution has given rise to mobile broadband technologies such as Long Term Evolution (LTE) defined by the 3rd Generation Partnership Project (3GPP), delivering high-speed access, data throughput (up to several hundred Mb/s) and low latency (<10ms) enhancing operational effectiveness and cross organization coordination by complementing existing narrowband communication networks.

With a high-speed broadband communication network, we supplement existing narrowband networks by adding eyes in the form of sharing real-time video feeds or high resolution images between all end-users in the field. Advanced analytics for object and personnel identification can be applied to assist police officers in crime-fighting. A high capacity data communication network allows large amount of data from data sensors on-board sophisticated systems to be sent in shorter intervals for more precise monitoring, providing a more effective mechanism for preventive maintenance.

LTE, Next Generation Critical Communications

LTE has emerged as the global standard for the fourth generation of mobile multimedia (voice, data and video) broadband communications since its definition by 3GPP more than a decade ago. Massively deployed worldwide for the commercial market, it has now been made available to the public safety community.

Offering interoperability with existing narrowband systems already deployed by the public safety community for decades, LTE has emerged as the answer to enhancing operations with advanced multimedia services, multimedia mission critical applications, providing maximum support for their day-to-day as well as large-scale events and emergency operations. Utilizing broadband technology has paved the way for a broader range of devices, from smart sensors to smart handheld devices such as smartphones and tablets, offering public safety users the capability to do more and do better.

> *As such, LTE has been referred to as the successor technology for TETRA, DMR and P25. Furthermore, starting from 3GPP Release 13, LTE has evolved as a suitable mission-critical-grade system with the initiation of the SA6 workgroup for Mission Critical Services (MCS).*

3GPP has initialized notable work items for SA6 including Mission Critical Push-to-Talk (MC-PTT), utilizing Group Communication System Enablers (GCSE) for highly efficient group communications over LTE, Proximity Services (ProSe) and Isolated E-UTRAN Operation for Public Safety (IOPS) or base station fallback mode for enhanced network reliability. Mission Critical LTE has emerged as an industry standard for mission critical users (public safety) as well as business critical users (public utilities, transportation, etc).

The frequency spectrum of commercial LTE networks by Mobile Network Operators (MNOs) covers a wide range from 450MHz to 3.5GHz, accommodating different channel bandwidths from 1.4MHz to 20MHz and different duplexing modes (FDD and TDD). Dedicated and private LTE networks may utilize a subset of the wide spectrum that is below 1GHz, such as 450MHz (Band 31), 700MHz (Band 14 and Band 28) and 850MHz (Band 26), with a bandwidth of 3 + 3 MHz, 5 + 5 MHz or 10 + 10 MHz. The recommended bandwidth is 10 + 10 MHz considering the scale and capacity of networks for public safety. The first countries that have been quick to move include the United States (Band 14), South Korea (Band 28), United Kingdom and Middle East.

LTE communication networks are based on an all-IP architecture. This allows for network reliability features such as local and geographical redundancy, preventing single-point-of-failure, providing the high availability required by public safety end-users.

Furthermore, LTE technology features guaranteed and differentiated end-to-end Quality of Service (QoS) and priority/pre-emption mechanisms to ensure service availability for the most critical applications and end-users.

LTE systems are armed with self-optimizing network capabilities to allow for simplified maintenance. This enhances LTE systems with scalability and fluidity in networking.

However, PMR operators migrating to LTE will need to address some challenges to reap the benefits. Frequency resource is scarce. Governments are facing difficulty in re-farming and re-allocating frequency spectrum for the deployment of private LTE networks. Even so, priority will be given to public safety organizations in most countries.

Mission Critical standards for LTE are still a couple of years away from attaining the full suite of mission critical features to guarantee a full change-out of existing PMR infrastructure.

Therefore, public safety organizations are more in favor of PMR and LTE interoperation, maintaining their current level of operations while preparing for the benefits of mission critical broadband applications.

Furthermore, outright replacement to a full private LTE infrastructure requires massive capital investment. It is important for public safety organizations and governments to strike a balance.

Subsequent content of this paper aims to provide guidelines to achieve this through the proposal of infrastructure and business models.

Mission Critical Applications over Operator's LTE

Availability of frequency spectrum has presented an uphill task in the deployment of private LTE networks, even for public safety organizations. With MNOs holding a much wider spectrum and existing infrastructure already built-up, partnership with MNOs prove a viable option to balance feature with initial investment. Making use of existing infrastructure significantly shortens the time required for a mission critical LTE network to be up and running.

MNOs are also drawn by the fact that the market for private LTE infrastructure is growing and they can capitalize on this growth by offering their existing infrastructure to governments to grow their revenue. Furthermore, MNOs have the priority in most cases to obtain newly released spectrum by government-led projects for public safety projects. With more frequency resources, MNOs can generate more revenue as they are also free to allocate part of the new frequency band for consumers.

> *In the United States, the First Responder Network (FirstNet) Authority and MNO, AT&T formed a partnership whereby the government will provide the frequency spectrum while AT&T will jointly invest, deploy, operate and maintain the network, providing a network designed for public safety*[1].

In the United Kingdom, the Emergency Services Network (ESN) is built on MNO EE's Radio Access Network (RAN) shared by both public safety end-users and consumers, with public safety end-users using a dedicated core network.

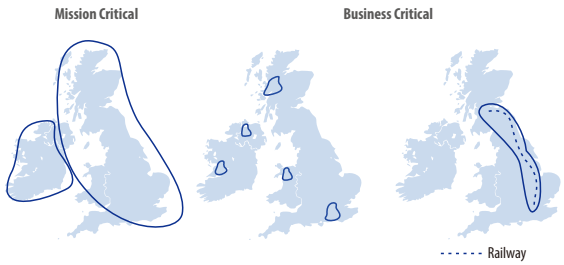
Countries such as France, Australia and New Zealand are following the approach of these three countries.

This precedence serves to provide a lifeline to public utilities, transportation and mining industries wishing to enjoy the benefits offered by a mission critical broadband communications network.

Existing infrastructure by MNOs however, remain largely for consumers while mission critical and business critical users require enhancements on availability, reliability, security and functionalities such as command and dispatching.

Radio coverage is required to be extended to provide services to even sparsely populated or non-populated areas due to the very nature of public security operations. The number of users served range from tens of thousands to hundreds of thousands depending on the size of the country. 100% service continuity is expected during major incidents and crisis. Higher levels of data security and protection against malicious attacks are of utmost importance. Therefore, hardening of the commercial network is necessary while the advantage for MNOs is that, this hardening is beneficial and attractive to their consumers as well.

For the business critical segment, these requirements are typically concentrated on the actual location of the business with the number of users served limited by the size of the organization business owners often looking to balance performance and investment and are generally not as stringent as public safety end-users. Coverage requirements for railway transportation applications is a classic example of having coverage where needed (only along railway tracks).



Business Models

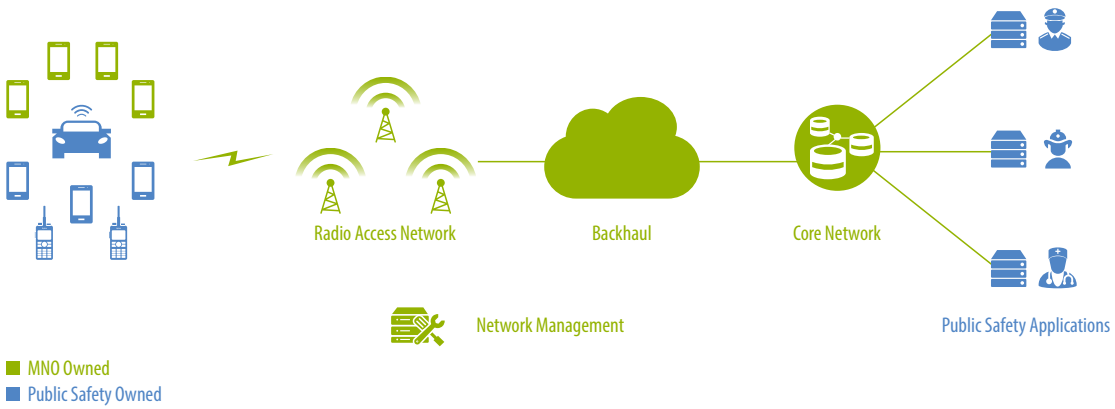
In this section, the white paper discusses the different business models with which governments, business organizations and MNOs can collaborate and their benefits to the mission critical and business critical segments as well as to MNOs.

The provision of mission critical services for public safety authorities are typically managed by a government-controlled organization. This organization can be a government-owned operator, a government body or even a private company with a service agreement with the government. This organization oversees the maintenance of the network and services.

For public safety users, they need to be able to entrust the service operator with critical and highly confidential information. The operator must be able to ensure confidential information is not leaked out to un-intended and unauthorized parties, at the same time providing high service availability required by mission critical operations. For example, push-to-talk services getting immediate connection to the network the very moment the PTT button is pressed. Accountability to user organization is established by a Service Level Agreement (SLA). In most countries, legislation can be involved to detail the authorities of the service operator.

Overlay: Mission Critical Applications over MNO Core

In this business model, the public safety agency (police, fire brigade, ambulance) simply deploys their application servers on the operator core network, sharing the same coverage and spectrum with consumers. The public safety agency enters into a service contract with the MNO and pays a consistent and periodic data subscription fee in a pay-as-you-use manner. Public safety end-users can use their own LTE devices.



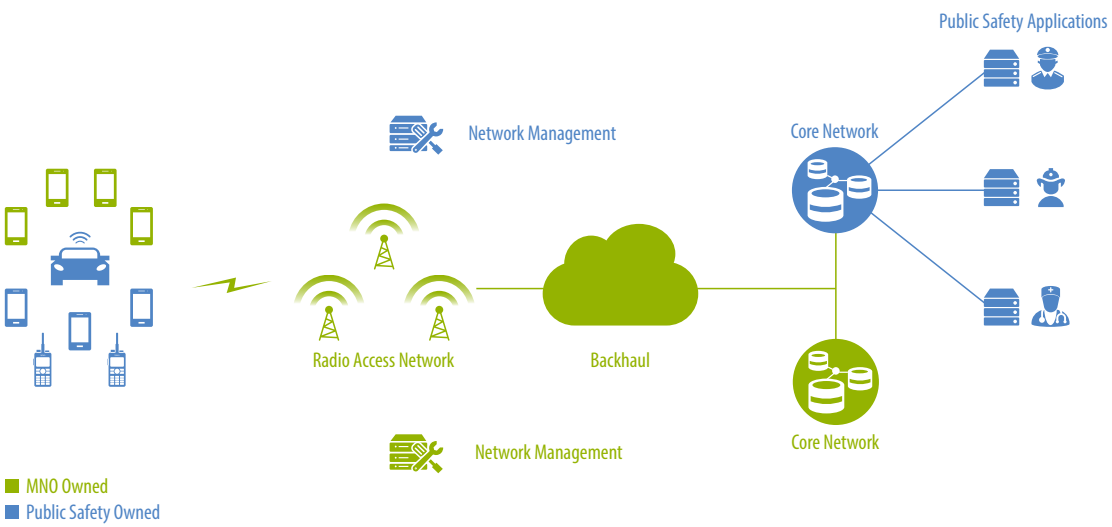
The advantages of this model to MNOs is obvious as they only need to provide regular maintenance in a similar manner to how they are already managing their consumers. For public safety agencies, this will prove to be relatively inexpensive if the LTE infrastructure is well in-place and data traffic is well managed and if rugged devices procured can be used within the assigned commercial spectrum. CAPEX will involve only the application servers and terminals while OPEX will consist of the monthly data subscription fees. Network upgrading costs are the responsibility of the MNO, which is responsible for resolving all technical issues and ensuring the appropriate level of service. The setup time for public safety agencies is almost nothing, as the MNO network can be available almost immediately.

The challenges for this model for public safety agencies include having no control over coverage, availability, service prioritization and resilience. Coverage is usually limited in sparsely populated areas, leading to gaps in coverage in rural and isolated areas. There is little or no support for mission critical features. This can be addressed by SLAs to mandate the implementation of priority access and network redundancy. These will come at a cost to ultimately impact the OPEX for public safety agencies. Implementation of service prioritization require specific network interfaces on the MNO Core Network to be open for integration with the mission critical applications. In most cases, the MNO Core Network and RAN will require upgrading to provide end-to-end service prioritization and mission critical services. These additional upgrades for mission critical and sometimes business critical end users, require substantial CAPEX for MNOs.

Service from a Mobile Virtual Network Operator (MVNO)

The MVNO business model first surfaced in the commercial sector, where MNOs lease out part of their spectrum to a private company or a private operator who is referred to as an MVNO. A popular example is Virgin Mobile in the United States, leasing spectrum from T-Mobile. MVNOs usually provide value-added services such as enhanced video streaming for users opting specifically for such services, providing their own SIM cards, branding, marketing and customer service in a similar fashion as MNOs.

This model is based on the concept of network sharing released by 3GPP in two documents: TR 22.951[2] and TS 23.251[3]. TR 22.951 titled "Service Aspect and Requirements for Network Sharing" describes deployment scenarios, network operator and user requirements and other considerations for network sharing solutions[4]. This document also lays down fundamental principles, such as avoiding the need for proprietary terminal devices to benefit from network sharing, the requirement to support legacy terminal devices, the need to allow service differentiation between shared network operators, and avoiding compromises to the services offered in shared networks. TS 23.251 defines the architecture and functions needed to allow several core network operators to share a single RAN, in order to meet the requirements of TR 22.951. TS 23.251 sets out two approaches to sharing the LTE RAN, highlighting the differences in the core network aspects illustrated below:



Multi-Operator Core Network (MOCN)

With the MOCN approach, the public safety operator will build a dedicated core network for public safety users to share a common RAN with the commercial operator. This is often referred to as RAN Sharing. With this approach, public safety agencies can manage an isolated network with their own user and device management system, implement end-to-end service control and prioritization and data security to get access to guaranteed and secure broadband data services over the MNO LTE access network for clearer service differentiation with commercial users. With a dedicated core network, public safety agencies are able to achieve interworking with legacy networks and support roaming. Network construction costs are significantly reduced when base station and frequency resources can be shared.

Gateway Core Network (GWCN)

With the GWCN approach, the network operators (public safety and commercial) also share the Mobility Management Entity (MME) network element of the core network. The MME network element is responsible for bearer management and connection management between the terminal devices and the network. Sharing the network element results in additional cost saving compared to the MOCN. However, this approach will lose the level of differentiation provided by the MOCN between public safety and commercial operators.

In both approaches, coverage expansion by the addition of new base stations or service upgrades to existing base stations will result in re-configuration of the core network and the network elements, which will incur additional maintenance costs.

Public-Private Partnership Project (PPP)

The PPP is the much preferred business model for public safety agencies, featuring a dedicated and standalone network, deployed, operated and maintained by the MNO or a government assigned independent operator. This MNO assumes the financial, technical and operational risk of the network. With this heavy responsibility, the MNO in this model is typically one of the largest telecom operator of the country. Public safety applications and terminals shall still be the responsibility of the public safety agencies. The First Responder Network (FirstNet) of the United States is based on this business model with AT&T as the network operator, responsible for building additional base station sites in rural areas.

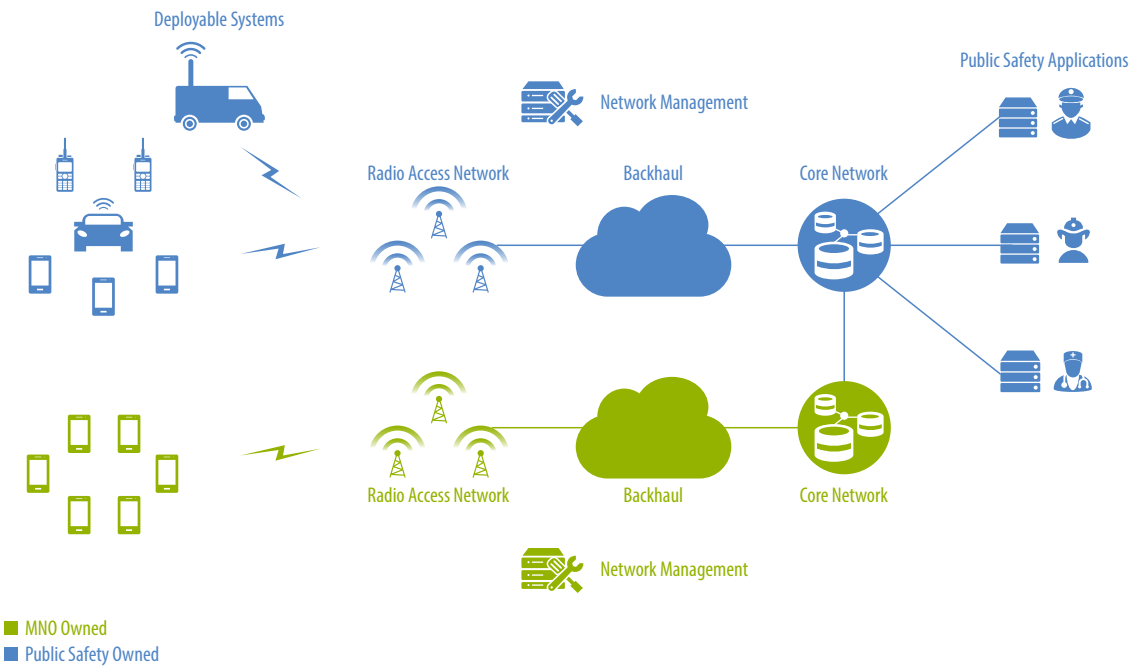
The key benefits of the PPP model are that public safety agencies are the sole users of a full mission critical LTE infrastructure, with their customized communication requirements fulfilled and have full control over coverage, resiliency and service prioritization. The MNO for such as network usually enters into a partnership with a technical solutions provider for the above mentioned requirements. Deployable LTE systems for emergency operations can be used to enhance the capabilities to cope with sudden surges in capacity requirements for major events or unplanned events.

With full control over the base station sites, backhaul and applications, the network can be fully optimized and CAPEX and OPEX can be reduced. Excess network resources can be sub-leased to business critical owners such as in public utilities and transportation industries, pretty much the reverse compared to the MVNO business model. In more extreme cases, the public safety authorities can have full ownership of the network, taking full responsibility for the network elements, hardware and software. For the public safety authorities and agencies, they will now have an LTE network fully designed to match and fulfill all of the public safety requirements, tailored to specialized missions unique to their operations. Future system evolution roadmaps can also be strategized and adjusted according to the requirements of the public safety agencies.

The first and foremost challenge for public safety authorities and agencies will be on the financial side. Owners of a PPP network are looking at huge initial investments on a dedicated infrastructure, new systems and applications and time commitment as the involved civil works will impact the in-force date of the next generation system. For large scale deployment, this project will need to be planned in phases and over multiple years, with deployment in critical areas being prioritized. The next challenge will involve the valuable frequency resource. Clearing the designated spectrum of previous allocation and services is usually a slow process with the country government playing a key role in facilitating the re-farming. If the designated frequency spectrum for usage is not supported by a mature industrial chain, public safety agencies could face issues in the procurement of terminal devices. These challenges translate to additional CAPEX. Implementation of the PPP model requires carefully planned budgeting and financing.

Hybrid: Combination of MVNO and a Private Network

In view of the deficiencies of the Overlay and MVNO models and the challenges involving the implementation of the much-preferred PPP model, public safety agencies can opt for a MVNO plus PPP hybrid model. This model aims to provide a balanced approach to reap the benefits of both the MNVO and the PPP models.



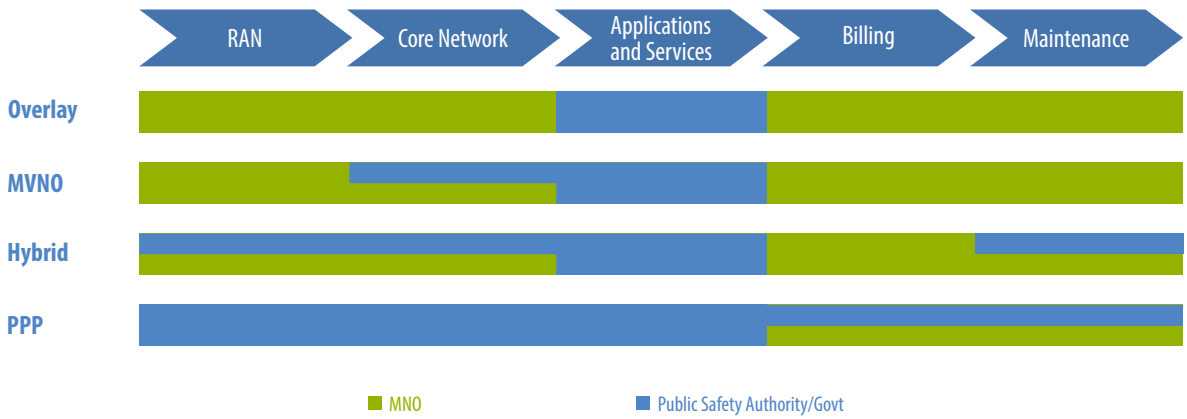
Spectrum resource can be leased from MNOs similarly to the MNVO model. What is different with this model is that the public safety agency will now build their own base station sites in critical areas (usually sub-urban and rural areas where the MNO do not build base station sites), aside from building their own Core Network and public safety applications. Backend mobile office applications that are less critical can still be on the MNO owned RAN, with the MNO Core Network interfacing with the Public Safety owned Core Network for controlled access to the public safety applications. Deployable systems can be introduced into public safety operations.

This model is relatively easy to implement in the early stages of building the basis for the next generation communication platform with LTE being a matured technology for both the commercial sector and mission critical services. This model preserves benefits such as network scalability for high traffic and user volumes, having retaining full control in the service prioritization aspect with a dedicated mission critical Core Network in emergency situations. Starting small with the building of dedicated private base station sites also allows the public safety agency to manage a phased upgrading, expanding the coverage of the private network portion when frequency spectrum becomes available in time. With the availability of both the MNO network and the private network, non-mission critical traffic can be offloaded to the MNO network, preserving resources in the private network for traffic surges in the occurrence of major events (natural disasters, large-scale incidents) and emergency situations.

Implementing a hybrid model introduces greater complexity in the technical design, operations and financial aspect, requiring critical consideration and coordination between the MNO and private network, not forgetting a carefully negotiated SLA with the MNO. The interfacing and integration between the MNO and private network also requires a high level of technical expertise. Although there are still issues with coverage, security and reliability yet to be fully resolved, the hybrid model represents an option for public safety agencies to strike a balance between investment and operational capabilities.

Summary

The responsibilities of the MNO and public safety authorities for the business models discussed above can be summarized in the diagram below:



The comparison of the benefits by considering CAPEX, OPEX, coverage, capacity, scalability, security, control and public safety features for the business models can be summarized as follows:

	CAPEX	OPEX	Scalability	Security	Control	Public Safety Features
Overlay	Low	Low	N/A	Weak	Weak	N/A
MVNO	Moderate	Moderate	N/A	With dedicated equipment	With dedicated equipment	With dedicated equipment
Hybrid	Moderate	Moderate	Dedicated Resources	Dedicated Network	Dedicated Network	Dedicated Network
PPP	Moderate to High	Moderate to High	Dedicated Resources and Network with Full Isolation from Commercial Network			

The choice of business model depends on many factors including those discussed above. Public safety agencies need to consider the change in user habits and conduct of operations. Public safety operations require clear definition of services and service levels for each processes. Therefore, a trusted solutions provider or partner with highly qualified technical personnel and solutions expertise to validate that the new system will meet all the requirements of public safety end users, ensure that all terminal devices, applications and all components of the solution are working properly and to test the end-to-end solution comprehensive during the design and implementation phases. Public safety agencies are charged with the sole mission to protect the lives and properties of the public and their very own public safety responders. They require the latest capabilities and technologies that has been thoroughly tested and ever ready for this purpose.

To strike a balance between investment and capabilities, the MVNO approach is most recommended.

It is a recognized fact that most nations are not expected to be allocated dedicated spectrum for nationwide deployment. Therefore, choosing a model where the existing infrastructure is left relatively untouched while focusing on interfacing and integration between networks with dedicated application servers and end-to-end service differentiation puts less financial stress on MNOs and government agencies. Government and public safety agencies can rely on established mission critical system, application and solution providers to benefit from the extensive coverage provided by MNO coverage and the hardened solutions tailored for their business needs.
In the next phase of upgrading, public safety agencies can then transit to the Hybrid model, by setting up additional base stations for coverage in hotspot areas with surges in data traffic demands or in rural areas not covered by existing base stations built by MNOs. Public safety can now have on-demand deployable systems for emergencies and contingencies, resulting in a communication network with more scalability.

Public safety agencies need to implement a business model for them to enjoy the benefits of mission critical broadband services fast as well as a basis for them to continue to upgrade and enhance their capabilities. The successful reference of UK's ESN, implementing the MOCN variant of the MVNO provides a great example for other nations and MNOs.

Hytera: Enabling Mission Critical Applications over Operator's Network

Hytera has amassed over two decades of industry experience, having partnered with PMR operators globally, not only in the public safety industry but also in public utilities, transportation, oil & gas, etc. Having foreseen that the successor technology to PMR will be LTE-based, being the leading solutions provider for two of the mainstream PMR technologies (DMR and TETRA), Hytera has gone on to develop a full suite of mission critical LTE products and applications tailored for both mission critical and business critical users.

Hytera offers technical solutions and expertise to partner MNOs for all of the four business models discussed above, with a product portfolio covering infrastructure, devices, applications and services based on multiple technologies including PMR and LTE. Compliant with 3GPP Release 13 and above, Hytera's LTE solution is able to offer full Mission Critical Services over commercial Core Networks (for the Overlay business model), dedicated and private Core Network for integration with commercial RAN (MVNO and Hybrid business models) and the full product suite including applications and terminal devices for the eventual implementation towards the PPP business model. Hytera's network management system (NMS) and device management system (DMS) for terminal devices, with a mechanism similar to the hierarchical organizational structures that PMR networks had been built on is tailored for the operational models and workflow processes for public safety authorities. The NMS and DMS is able to manage both existing PMR and next generation mission critical LTE systems and terminal devices on a single platform and from a single point.

Hytera is armed with technical expertise to allow mission critical broadband services to handover between the commercial network and the dedicated private network using the standard 3GPP compliant roaming interface between both networks, providing a highly scalable and flexible communication and networking solution that can be evolved to future technologies. This solution is also capable of inter-operation with existing PMR systems.

Benefits to Public Safety Agencies

Hytera's next generation critical communications solution provides the following features and capabilities for public safety agencies and end-users, enabling them to work safely and more efficiently.

Network Control and Management

The operator is always in control of network resources:

- Allocating access and resources to authorized subscribers
- Ensuring subscribers stay securely connected to one another and to the access network
- Only subscribers holding authorized USIMs issued by Hytera are allowed access to the network. This capability is an in-built functionality of all 3GPP compliant networks.
- USIM authentication keys, encryption keys and subscribers will be under full control of the operator of the network

Security

- With the deployment of MCS application servers, data security is ensured for public safety users by implementing end-to-end encryption between public safety terminal devices and the MCS application servers over the commercial access network.
- Building a portion of the access network with dedicated and private base stations enhances network security further by providing physical isolation with the commercial network, eliminating the chance for intrusion or malicious attacks through the commercial network.

Resource Control and Device Management

- With the DMS, the critical communication network operator can set blacklist or whitelist for APPs to prevent unauthorized application usage and downloading or even set different access priority for users to APPs.
- The data policing feature available via the 3GPP-defined PCRF network element allows the operator to define user profiles and policy for each USIM and APN, limiting user bandwidth for different user profiles.

3GPP-Standardized QoS Management

- The critical communication network operator can manage and configure the service level Quality of Service (QoS) Class Identifier (QCI) for all subscribers and subscriptions via the PCRF. In the case where integration with the commercial Core Network is required, the RX and SGi interfaces need to be supported and available for integration.

3GPP-Standardized Mission Critical Services Features

- Hytera's LTE MCS solution is compliant with latest 3GPP standards, defined for Broadband Trunking capabilities, utilizing the enhanced feature, eMBMS (evolved Multimedia Broadcast Multicast Services) to provide fast and efficient group voice, data and video communication within a base station site as well as the whole network. Public safety end users of MCS can enjoy immediate multimedia communication with significant savings in air interface resources, support more user capacity and handle sudden surges in user capacity. This feature is crucial to public safety end users but not implemented for consumers in commercial networks.
- The IOPS (Isolated E-UTRAN Operation for Public Safety) feature enhances the availability and reliability of a network by initiating a fallback to an embedded core network module within an eNodeB when connection to the main core is disrupted or the main core fails. This feature provides public safety networks with the added reliability required that commercial networks do not support.

Cross Technology Inter-Operation

- Hytera's critical communication solution allows for cross-technology inter-operation, offering public safety agencies a key proposition to retain their existing infrastructure for critical voice communication and enjoy value-added broadband multimedia trunking data and video communications for enhanced operational effectiveness.
- Implementation of a single unified NMS and DMS for multiple communication networks allows for single point management, greatly simplifying the maintenance of devices and equipment within the network.

Customizable Integration Platform

- Hytera's solution provides strong integration support for public safety agencies to implement their selected radio interface encryption and authentication mechanisms by vendors of their choice.
- Public safety agencies can integrate their own third party applications and sub-systems (such as existing CCTV systems) into the network conveniently.
- Command & control and call taking systems can be fully integrated with the multi-technology communication network to enable cross-agency coordination, enabling unified control for quick response and large scale operations.

Value Proposition for MNOs

The MVNO approach is seen as a viable option for the eventual transition to a dedicated mission critical broadband infrastructure considering the financial risks and technical challenges. It is seen as the next step in smart policing, arming public safety agencies with advanced technological tools to match up to modern methods of criminals in creating disruptions to public security.

MNOs can play a big part in providing public safety agencies with the broadband communication infrastructure as a basis for them to start building the capabilities, starting trial programs early. The upgrading process is not merely the procurement of terminals and equipment, public safety agencies will also need to engage solution providers or partners, such as Hytera, with their technical expertise and experience to understand the issues and also manage the security, reliability and inter-network and inter-systems integration to materialize the desired outcomes.

MNOs can leverage on the expertise of solution partners to open the doors to business critical industries who have the same requirements, expanding their business opportunities.

MNOs should start laying the groundwork for offering their services to beyond commercial users.

Hytera is ready today, to work with MNOs and help public safety agencies and business sectors bring mission critical broadband solutions into use.

References

1. First Responder Network Authority, Official Website of the United States Government – "https://www.firstnet.gov/network"
2. 3GPP TS 22.951 v15.0.0 released on June 2018 – "Service Aspects and Requirements for Network Sharing"
3. 3GPP TS 23.251 v15.1.0 released on September 2018 – "Network Sharing; Architecture and Functional Description"
4. 3GPP Network Sharing Enhancements for LTE – https://www.unwiredinsight.com/2013/3gpp-lte-ran-sharing-enhancements

Hytera
Respond & Achieve

Hytera Communications Corporation Limited
Stock Code: 002583.SZ

Address: Hytera Tower, Shenzhen Hi-Tech Industrial Park North, Beihuan RD.9108#, Nanshan District, Shenzhen, P.R.C.

Tel: +86-755-2697 2999 **Fax:** +86-755-8613 7139 **Post:** 518057
Http: //www.hytera.com **marketing@hytera.com**