masonadvisory

WHITE PAPER

June 2018

IS COMMERCIAL 4G READY FOR MISSION-CRITICAL SERVICES?

Opportunities and challenges: entrusting critical communications to public mobile

Mission-critical services (MCS) are predominantly served by private mobile radio (PMR) systems, which provide efficient command-and-control voice services and short data messaging, but lack the broadband capability required for the modern mobile workforce. Many of the systems in use by public-safety, utility, and emergency services are augmented by use of 4G data services from commercial mobile telecom operators (CMTOs), without the resilience of a PMR system. With the recent advances in 3GPP standards, some MCS are now moving over to public 4G CMTOs.

CMTO networks offer in-the-field broadband and access to commercial off-the-shelf services and technology. But how do they measure up to PMR in terms of availability, resilience, and control for mission-critical communications?

This paper looks at the opportunities and challenges presented by moving mission-critical voice and data communications to a CMTO, and outlines the key considerations.

Cardinal requirements for mission-critical services

First requirement: availability

There are four cornerstones of service availability, whether via PMR or CMTO: coverage, latency, capacity, and prioritisation.

Coverage

Mission-critical communications must be available at all times and in all areas where users need to operate. With a public mobile network, the requirement for comprehensive geographical coverage could be met by selecting a CMTO which has a national roaming agreement with other operators, or by using a dual-SIM device with least-cost routing across two CMTOs. However, neither arrangement would ensure coverage in locations such as tunnels, which require specialist solutions.

Profit-driven CMTOs may question whether the return from MCS is sufficient to justify the cost of the service enhancements and additional infrastructure, such as extra base stations, that it demands. Extended coverage or specialist indoor solutions would primarily need to be negotiated with the CMTO, but lock-in to a single network also raises concerns since it would remove user flexibility to roam, even in circumstances where another network could provide a better service. Operator lock-in could be avoided through a model that enables the services to be separated from the network and enables connection to one or more networks with minimal disruption and a flexible commercial agreement. However, the augmentation of coverage required for MCS provides an opportunity to deliver a shared infrastructure commercial model which benefits the MCS and commercial users by providing wider and deeper coverage – outdoors and indoors.

Latency

Latency – the time delay before a response is generated and returned – has never been faster. It is getting quicker with each generation of technology as protocols are optimised for efficient, fast transfer of data. Public-safety services have a requirement for fast, seemingly instantaneous, call set-up – particularly for emergency calling and group calls. In addition, immediate, reliable messaging for dispatch and alerts such as 'man down' are essential.

The group call facility available with PMR is now an option over CMTO networks with the new standards catering for mission-critical push-to-talk (PTT). This service is used very effectively in the public-safety arena where large numbers of officers can be in a single call and controlled through the

About us

Mason Advisory is an independent IT consultancy that does things differently, matching technology know-how with commercial and business sense.

For over 20 years, organisations across the public and private sectors have trusted our consultants to provide strategic advice and assurance for their most critical projects.

We work with blue-light organisations in the UK and further afield, and we are currently a member of the Home Office delivery partner team for the Emergency Services Mobile Communications Programme.

chain of command. In 4G, the group call set-up is fast, but the 'idle mode' feature which enables the user to save power and extend battery life can slow down 'adds' to the end-to-end call. Call set-up times are, therefore, typically slower on 4G than a dedicated public-safety PMR system, however, it is fair to say that group call set-up will be fast enough to feel instantaneous to users.

Capacity

In times of high demand, during major incidents and planned events, mobile capacity must be available to support both MCS and commercial users. At the Notting Hall Carnival in London, for example, public-safety users would be vying with thousands of other people for capacity on the same network.

Before 4G, mobile was entirely unsuited to carrying mission-critical communications. It is Long Term Evolution (LTE) technology, on which 4G networks are based, which has brought public mobile into the MCS arena. Mobile capacity is determined by the density of base stations serving an area, along with the amount of spectrum deployed, and LTE Advanced Carrier Aggregation enables mobile network operators to speed up data transfers and increase overall capacity by exploiting fragmented spectrum allocations.

Despite network upgrades, there may still be times when capacity is saturated, which means mission-critical communications must be prioritised over commercial use.

Prioritisation

Not only must the CMTO give priority to public-safety users, it must also ensure MCS pre-emption, so that MCS operate immediately without human intervention.

Prioritisation and pre-emption for MCS are built into the 4G standard and in Release 12 (R12), MCS prioritisation is the first stage of 4G features now available in the vendor and operator ecosystem. The UK's new Emergency Services Network (ESN), for example, is designed to operate over R12 of 4G, and early test results show prioritisation and pre-emption are effective in enabling and maintaining mission-critical communications at times of extreme loading.

In congestion scenarios, commercial users are pre-empted off the network to allow unimpeded operation of MCS. The CMTO moves them to other frequency layers, through load balancing or 2G or 3G, in order to maintain service while at the same time ensuring that MCS remains on 4G.

Second requirement: resilience

Traditional mission-critical PMR networks are specifically designed for optimum resilience in terms of power and transmission, and to minimise single points of failure. In contrast, commercial wireless networks are designed to provide a return on investment, so are structured to maximise revenue rather than prioritise mission-critical aspects of the service. Resilience, security, and performance will vary between network operators.

It is therefore crucial to consider the underlying topology of the proposed wireless network and closely examine the resilience of each critical component in the service path, including core switch sites, core transmission, metro ring, backhaul, and radio sites. It is especially important to look at any third-party suppliers, such as the provider of backhaul transmission.

A key part of the strategic business case for public mobile is to analyse the current level of resilience of a potential operator and perform a gap analysis to determine the enhancements required to support mission-critical communications.

Third requirement: control

Control means the ability to control provision of:

- the assets used to provide the MCS
- access to the network and management of the service at all times.

With a private network, this control is assured, but with a CMTO it becomes more challenging. While elements of agreed levels of control can be built into contracts, any change of ownership may put this at risk, especially where ownership moves to an operator from a foreign country. The network used by public-safety organisations for critical operations, and which holds public-safety subscriber and encryption details, is no longer in the carefully chosen hands of the original partner. The contacts must have provision to protect the service and be agile enough to move to another service provider or operator, should the need arise, with assured continuation of service.

Increasingly there is consolidation of commercial networks where two operators share common towers meaning a selected CMTO solution may change to one which no longer meets user requirements. Preferential access to the network can be negotiated, but if this is based on service level agreements (SLAs), there is a risk that the network operator may at times find it financially beneficial to pay SLA charges rather than provide the contracted level of service. It is therefore imperative that service performance oversight is provided in near real time with the reporting and governance structure to ensure that the service is provided as contracted and any challenges are swiftly rectified. This service management aspect is key in ensuring service delivery and management during times of crisis.

Big benefits of a CMTO

The main advantage of providing MCS using a CMTO, is the benefit from an already established nationwide network with the following main attributes:

- access to latest 4G technology nationwide with regular network updates
- expertise in managing and maintaining a national modern broadband network
- access to the spectrum and the capacity that is provided now and in the future.

Another key driver is quicker access to the innovation of commercial services and technology that are available off the shelf or are easily adaptable for public-safety use, including:

- drones, with video
- wearables, such as heart-rate monitors and augmented reality
- video streaming
- consolidation of systems and technology (one device or network).

With CMTOs, MCS can take instant advantage of technology upgrades and innovation, enjoying access to a wider development community which is constantly working on better ways of doing things. The economy of scale that comes with public solutions ensures costs will be driven as low as possible.

With 4G also comes opportunities to enable:

- smarter working on the move
- real-time analysis of large volumes of data
- improved situational awareness.

Building a business case for CMTO

The main challenge with building a business case for CMTO is around timing.

The commercial network for full MCS is almost there, but not quite. In the UK, ESN is expected to be fully commercial before 2020, offering a full suite of MCS via a CMTO – a probable world first, although South Korea is also on course for achieving this. The full MCS standardisation and availability of COTS MCS systems should also be available by 2020.

Meanwhile, the many mission-critical communications on new or refreshed private networks will stay there, or perhaps deploy a partial CMTO solution, such as using public mobile for data services. In the USA, for example, FirstNet is establishing a nationwide interoperable mobile broadband network based on LTE, but the Department of Homeland Security sees it as initially supplementing rather than replacing PMR networks.

Most PMR networks focus on voice, but public-safety networks increasingly require data communications. Supplementary services could be arranged with a single CMTO, or with all national CMTOs via an agreement with a roaming operator – a mobile virtual network operators (MVNO) – with end-to-end encryption to protect sensitive data. In this instance, PMR would continue to provide voice services and to support the data relied on by mission-critical applications such as vehicle and person location systems, but the commercial network would carry less critical high-speed data applications.

A good example of this is the ASTRID MVNO in Belgium. ASTRID, the public-safety operator which has a TETRA narrowband national

network, has set up a data-only MVNO, working through a roaming partner into all four mobile networks for a comprehensive belt-and-braces coverage.

Whether looking at a hybrid operation or full outsourcing of mission-critical communications to a CMTO, the key considerations are the same.

The main factors to look at are:

- control and quality of service
- security
- spectrum costs/availability
- timescales and cost to implement
- in-house resources/costs
- efficiencies using broadband technology
- eco-system and technology refresh
- upgrade and maintenance costs

A summary of the pros and cons of outsourcing to CMTO are summarisied below.

Element	Pros	Cons
Cost	Potential efficiencies, economies of scale, and access to reduced labour costs (e.g. outsourcing).	Additional costs related to supplier profit. Supplier motivated to maximise revenues over contract life.
Spectrum	The spectrum that the operator owns will often be far more that the MCS, offering greater capacity.	Spectrum is a finite resource and 4G spectrum is expensive, even when considering the opportunity cost if 'reserved for MCS' by the government.
Finance	Suppliers raise capital, not the customer for network build. Cost is opex, as spending is based on consumption of services.	Cost of finance added to charges; customer could get lower cost of borrowing.
Quality	Access to quality facilities and specialist resources not available in house.	Provider's primary motivation is revenue rather than service quality.
Risk	Risk of successful service delivery is transferred to the provider.	Full risk transfer is not possible: the customer is affected if service fails.
Security	Mobile operator can integrate the function into an existing capability, reducing cost.	In full outsourcing, the provider has access to encryption keys and authentication, which may be a vulnerability.
Control	Provider can often offer greater resource than an in-house solution.	Provider may be taken over by another company.
Flexibility	Provider may offer more options/greater flexibility through larger scale in-house facility.	Contract barriers and supplier 'lock-in' can affect ability to adapt to changing organisational requirements.
Technology	Access to latest technology is faster as part of commercial model.	Fast changing technology creates risk and cost to ensure service resilience is retained.

Contact us

If you would like to discuss how we can support you please email contact@masonadvisory.com or call +44 333 301 0093.