TETRA + Critical Communications Association
14 Blandford Square
Newcastle upon Tyne
NE1 4HZ
UK
Tel: +44 191 231 4328
Fax: +44 191 245 3802

Mobile Broadband for Critical Communications Users

A review of options for delivering Mission Critical solutions

First issued by the TETRA and Critical Communications Association December 2013

Registered Office,
Richmond House, Broad Street
Ely, Cambridgeshire, CB7 4AH,
UK
Registration No.4155039 in UK
VAT Registration Number GB 755 4236 24

Forward

Society is changing and so is the role of Public Safety agencies as well as those with the responsibility of managing and maintaining our critical national infrastructure. One of the greatest changes relates to the use of mobile communications and the availability and circulation of information. Users of Critical Communications should have the right tools to perform an increasingly difficult job.

This document has been produced by the TETRA and Critical Communications Association (TCCA) as a publicly available document aimed at Governments, Regulators, senior Public Safety officials and other users for whom mobile communications is a critical element in providing safety services and protecting critical national infrastructure.

The TCCA believes in standards based technologies, harmonised spectrum and interoperable solutions delivered in an open and competitive market. Many of today's Mission Critical mobile communications systems are delivered on a nationwide basis, particularly for blue light services such as Police, Fire and Ambulance. Experience has shown that cross border interoperability enhances the ability of such services to respond to major incidents and deal with crime. This is especially true in areas of Europe where international borders are no longer policed and where cross border incident management is undertaken on a daily basis. Utilities also need nationwide critical communication systems and railways require national systems with, in some cases, international roaming.

This document provides an insight into some of the methods by which critical mobile broadband services can be delivered and is a sister document to the TCCA's Strategic Case for Mission-Critical Mobile Broadband. Both of these documents are available from the TCCA. Contact details can be found on the web site[1].

[1] TETRA and Critical Communications web site can be found at www.tandcca.com

Contents

Introduction

Those operating in the world of Critical Mobile Communications will be aware of the growing demand for mobile high speed data services suitable for a Critical Communications environment. In the 21st century it is a sad fact that citizens have, and use, more advanced technology than our emergency responders. Urgent steps are needed to bring high performance data services and devices to those that are responsible for the health, safety and wellbeing of the citizens of this world.

The Critical Communications Broadband Group (CCBG) is a working group of the TETRA and Critical Communications Association (TCCA) and is tasked with driving the development of common, mobile broadband standards and solutions for Critical Mobile Broadband users worldwide based upon the 4th technology generation of mobile communications, LTE. In so doing it has formed relationships with a wide variety of user groups that have common aims. It is working closely with the Standards Development Organisations relevant to this requirement, including ETSI and 3GPP.

The CCBG's goals are to enable all Critical Communications users to access their information systems, applications, etc. reliably, and at broadband[2] speeds, on their professional mobile devices, wherever they are and whenever they have the need.

The creation of the necessary standards and technology is only part of the solution; delivering services that take advantage of such capabilities in a timely, cost effective and affordable manner is also a significant task and this paper addresses a variety of possible implementation options.

Technology and Standards development take place over extended periods and the LTE standard is no exception. Consideration will need to be given to the timescales in which data services are required before matching these to the available technologies. The existing data capabilities of today's PPDR radio technologies such as TETRA (both Release 1 and TETRA enhanced Data Services 'TEDS'), Tetrapol and Project 25 (P25), as well as cellular GPRS, EDGE and 3G services, may provide interim solutions until full Mission Critical broadband services become available.

Initial releases of the LTE standard are intended to cover 'data only' services. It can be expected that future releases will also include voice services. Voice over LTE (VoLTE) that is designed for the consumer market is likely to be the first voice service available in the short term. However, group based, push to talk, secure communications including fleet management functionality, all of which are fundamental requirements of Public Safety and other Critical Communications users, will require significant standards effort and are likely to be some years away before they become a serious consideration for Critical Communications users.

[2] For the purposes of this document, mobile broadband is defined as data with a rate above 384kbit/s (based on UMTS being a broadband service)

Context

The TCCA's Critical Communications Broadband Group (CCBG) is developing a generic Strategic Case document that seeks to describe the business needs of users for critical broadband services. The intended audience for that document includes senior user representatives, regulators, government officials and others involved in the decision-making process for the provision of appropriate resources including human resources, funding and spectrum. It is designed to clearly explain why Mission Critical Mobile Broadband will become an important tool in the future and why it is essential that sufficient spectrum and other prerequisite resources are made available for such services to be delivered.

If the case for Mission Critical mobile broadband is established then the next issue to consider is how those services can be delivered. This subject is a complex issue in its own right with many different options and many influencing factors. This document attempts to address these options and provide the reader with high level information about the principle options available.

Scope

As previously mentioned, the provision of Mission Critical Mobile Broadband (MCMBB) services is a complex issue and one that is still developing. As such, this document does not attempt to be a definitive guide to MCMBB implementation options. It is the ambition of the TCCA to create a single common standard that can be used for the provision of Mission Critical mobile broadband solutions. However, due to the variety of existing Mission Critical networks and the timelines involved with future technologies, appropriate solutions and their evolution will clearly vary across countries, organisations and services. Interoperability across borders will be beneficial and the use of common standards will be an important pre-requisite to achieving international roaming that is affordable.

It should also be recognised that, whilst basic services can be common, different user groups will have different needs. Services such as group communication for voice and data, proximity services (Direct Mode) and database enquiries are common services used by many professional users. However, there may be other services that are specific to individual user types. For instance, encrypted communication could be seen as police specific, whilst the management of sensor networks to monitor water or gas are industry specific. Transport organisations will have a heavy reliance on real-time positioning information and patient telemetry could be a lifesaving tool for paramedics. All of these services may not be possible over all types of network bearers, due to the differences in service characteristics such as coverage, availability and security. However, as a guiding principle, the basic services used by different communities should, at the very least, be designed to be fully interoperable.

The purpose of this document is to describe some of the different options that may exist for implementing critical mobile broadband and to look at the advantages and disadvantages of each. It is intended that this information can be used as a resource for those involved in making decisions relating to their own particular circumstance.

Executive Summary

The advent of smartphones, tablet PCs and mobile computers has changed the lives of large sections of the population. Younger people in particular are growing up with the ability to access information wherever they are and whenever they want. It is understandable therefore that those who are looking after the health, safety and welfare of our citizens expect to have the same capability from their professional communications equipment.

The TETRA and Critical Communications Association is, through its Broadband working group (CCBG), seeking to drive the development of common standards and harmonised spectrum to make Mission Critical mobile broadband available to the emergency services, the Critical National Infrastructure industries and other institutions for which group based mobile communications are critical.

The TCCA has developed a Strategic Case document that looks at the justification for implementing mobile broadband capability for Critical Communications users. However, the methods and business models for implementing Mission Critical Mobile Broadband are numerous and complex, especially when considering the forecast roadmap for standards development to create this capability and the uncertainty over harmonised, dedicated broadband spectrum.

This document accompanies the Strategic Case document by addressing the issues of how to deliver a Mission Critical Mobile Broadband capability. The document reviews the principle options and looks at how combinations of these options may provide a gradual migration towards a comprehensive capability. Individual options may be more or less advantageous based on local and often varying circumstances. The information provided herein is designed to assist users consider the options that are available to them and how they might relate to their particular circumstances.

An important consideration is whether there is an intention to complement their existing voice network with an additional broadband data capability or whether to replace the existing voice system with a single unified broadband network that combines both voice and data.

Whilst the single network approach might have certain attractions, the required standards and product development work is still in its early stages, especially for Mission Critical group based voice, data and video services. Users may feel that the risks of basing a future communications network on a technology whose development path is still uncertain are just not acceptable. In this case it may be better to implement data and video services alongside the existing voice network until such time as the voice capability is fully standardised and proven.

This paper addresses four principle options for the implementation of a mobile broadband capability:

- Take service from standard commercial networks
- Operate as a Mobile Virtual Network Operator (MVNO)
- Take service from a commercially owned dedicated network
- Build, own and operate a dedicated network

In addition, this paper considers a number of hybrid or combination approaches.

Take service from standard commercial networks

Taking service from an existing commercial Mobile Network Operator (MNO) is the simplest and possibly the cheapest option for obtaining basic data services. Some organisations will already have a relationship with one or more commercial providers. For Mission Critical users it will be necessary to negotiate appropriate Service Level Agreements (SLAs) to ensure that minimum standards of coverage, capacity, availability and resilience are committed to. Commercial networks already exist in many countries and the user can take advantage of standard commercial terminals as well as some specialist devices. Users can now be provided with access to additional information that improves their effectiveness whilst away from the office.

The primary disadvantages of this arrangement are that the user organisation has no real control over the coverage, availability or resilience of the network and performance will typically be on a 'best endeavours' basis. Standard commercial networks tend to have little resilience; with downtimes of several hours not uncommon. Outages of more than 24 hours have been reported[3].

Current networks do not offer Group Calls, Direct Mode capability (calls made without access to the infrastructure) or other PMR style functionality. The operator may or may not be prepared to commit to adding such functionality later.

At times of major incident, commercial networks tend to become overloaded and congested. Some operators have agreed to provide priority access to the network when required. There is little experience so far of how successful this priority access will be when the network is under stress.

If the network is being used for non critical, data-only services these limitations may be acceptable in today's environment. But many users anticipate that mobile data applications will become Mission Critical in the future. Experience shows that in large cities, network congestion can be a problem even during normal circumstances and this may inhibit Critical Communications users from relying on such a network for non mission critical applications.

Operate as a Mobile Virtual Network Operator (MVNO)

MVNO arrangements are a well-established principle in the commercial network arena. The MVNO makes an arrangement with one or more MNOs to buy access and capacity for their own customers. The MVNO brings the knowledge and expertise of the users' requirements and takes on the role of managing the end users, managing access to the network and taking care of any billing requirements.

The MVNO model enables existing TETRA/Tetrapol service providers to maintain the relationship with their users and act on their behalf to negotiate dedicated services through a Service Level Agreement (SLA). The MNO has the benefit of not having to deal individually with the demanding requirements of the individual users. The MVNO arrangement can be seen as the first part of a longer term hybrid solution described later in this document.

As with standard commercial networks, the MVNO solution will only provide service where the operators have installed coverage and network resilience levels may only be that which is considered

[3] e.g. Blackberry outage October 2011
see http://www.reuters.com/article/2011/10/12/us-blackberry-idUSTRE79B24Y20111012

necessary by the MNO for commercial services. During a major incident, commercial networks tend to become overloaded and congested.

Some Mobile Network Operators have agreed to provide priority access to their network when required. However, there is little experience so far of how successful this priority access will be when the network is under stress.

Take service from commercially owned dedicated network

In this solution, one or more Mission Critical user groups contract with a commercial organisation to build and operate a dedicated network. Since the network is dedicated to Critical Communications use it can be built to meet the required level of coverage and availability, and the users can exercise a higher level of control over the network and the operator. Future functionality can be specified at the outset ensuring the Mission Critical functionality can be provided as soon as it becomes available.

The significant advantage of this solution is that only Mission Critical users will take service from the network. Control can be exercised as to priorities of access, and there are no commercial users to take capacity during an incident. Since the network is being built for Mission Critical users, their requirements in terms of coverage, availability and resilience can form part of the contract. Some elements of the network such as antenna sites and backhaul may be shared with commercial cellular operators to reduce infrastructure costs.

To create a viable business case it will be necessary to make a long term commitment to a single provider. 10-15 years is a likely minimum. Dedicated networks can only be deployed if suitable spectrum can be obtained or accessed. At this stage no dedicated harmonised spectrum has been set aside within Europe, but spectrum allocations have been made in the US, the Asia Pacific region and in parts of the Middle East. Decisions on spectrum are expected in Europe over the next 2-3 years. Network build timescales will be longer for any form of dedicated network when compared to the use of existing cellular networks. Within Europe, subject to spectrum availability, dedicated networks could be expected from 2018 at the earliest.

If harmonised spectrum is available, cross border agreements between users of neighbouring countries can be negotiated, without involving third party operators, and encryption mechanisms can be shared easily.

Build Own and Operate Dedicated Network

In this solution the user builds, owns and operates a dedicated network. The network can be dedicated to one particular user organisation, but would probably be dedicated to a number of Critical Communications user organisations such as Police, Fire, Ambulance, Utilities, etc. Since the network is dedicated to Critical Communications use it can be built to meet the required coverage and availability criteria, and the users will have absolute control of the network.

This model is typical of Public Safety solutions in many European countries that have built, owned and are operating their existing Mission Critical voice networks. In most cases a pseudo independent company is created by the Government to take responsibility for the build and operation of the network.

The primary advantage for this option is that the users and their respective Government have full control over the procurement process, the network procured and the operating assets; as well as the coverage, resilience and functionality of the network.

In common with the previous model, if harmonised spectrum is available, cross border agreements between users of neighbouring countries can be negotiated, without involving third party operators, and encryption mechanisms can be shared easily.

In today's economic climate, funding of dedicated new build networks is challenging and lack of suitable spectrum in some regions of the world make it very difficult to deploy such a network. Users may decide to opt for an alternative solution as an interim measure until economic conditions improve and whilst spectrum issues are resolved.

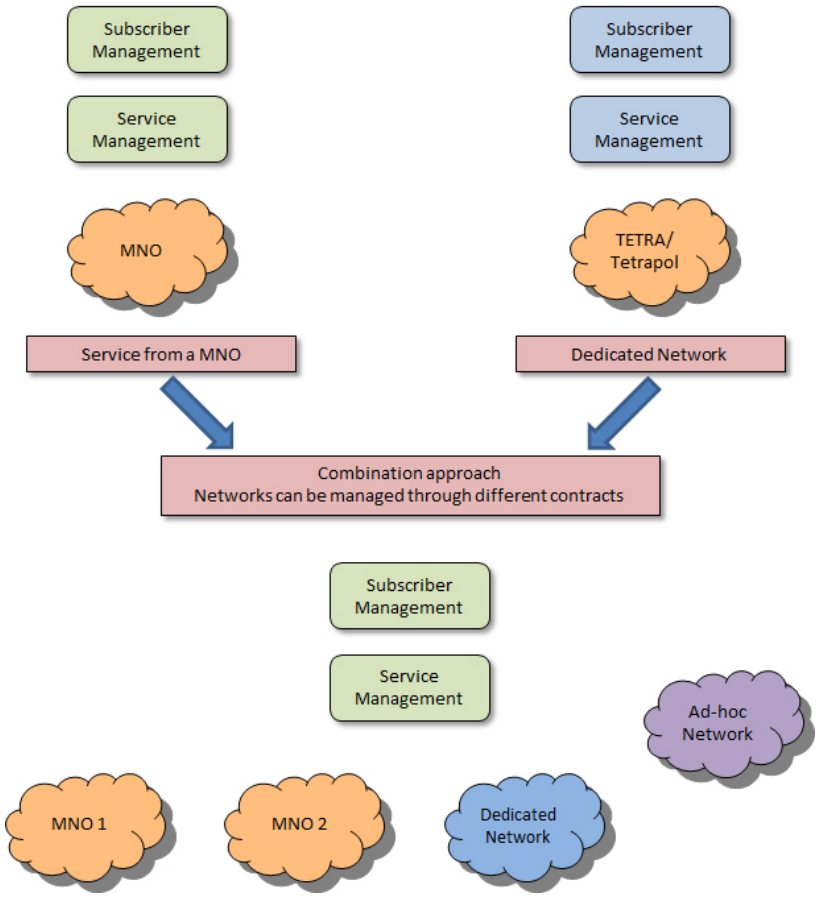
A Combination Approach

In looking at the available implementation options, a user/operator may conclude that none of the options described above adequately meets the need in their particular circumstances. However, a combination or hybrid approach may provide the best compromise. As previously mentioned and, as an example, the market availability of dedicated systems may be too far in the future. An alternative solution for the most important geographical areas may be an acceptable starting point.

Some use of a MNO/MVNO based solution, providing service on a best endeavours basis, has the advantage of early deployment and lower initial costs. Experience of the benefits of mobile broadband services will enable users to decide what long term advantages there are from use of the technology, whilst funding and spectrum issues are resolved and whilst full Mission Critical capability is developed by the standards makers and industry.

Private systems may be deployed to fill in coverage gaps where MNOs do not consider it viable to provide infrastructure. Private systems could also be deployed to enhance capacity in areas of high demand. A combination of private and public systems could provide users with dedicated systems where traffic levels are high and use public networks for occasional traffic.

A combination approach enables agencies to benefit from access to broadband services whilst waiting for the full Critical Communications functionality to become available. However, any approach that is based on multiple solutions will inevitably require more resources to manage and greater expertise to bring these solutions together. Combination approaches are already utilised by many organisations and, in some cases, may prove to be more expensive as individual contract values will be smaller.



Combination Approach

FirstNet

In the USA, the Obama administration allocated 2 x 10MHz of spectrum and US$7 billion to stimulate the roll out of a nationwide Public Safety network. With funding and spectrum already in place the US has significant momentum to provide Public Safety users with a mobile broadband capability. The Government set up an organisation called FirstNet to take responsibility for this initiative. Planning and decision making are at a very early stage but the indications are that the eventual solution will be based on a hybrid solution involving one or more existing commercial network operators.

The National Public Safety Telecommunications Council (NPSTC), which is a user representative body, is recommending that investment in existing voice networks is maintained and that FirstNet is initially used as a data only network.[4] It is their view that Mission Critical voice services will not be available and proven for at least 10 years.

The Role of Satellite Services

Satellite services are able to provide Public Safety users with communications over very wide areas and are therefore particularly well suited to locations hard to reach or justify with terrestrial networks. Existing spectrum in the 2GHz band (S-band) provides an option to the Public Safety sector to implement a "commercially owned dedicated network" approach relatively quickly. A terrestrial network can be deployed in areas where higher capacity is needed whilst rural areas can be covered by satellite services.

With the issue of spectrum for Critical Communications users still uncertain, the development of a dedicated network using the Mobile Satellite Service (MSS) S-band spectrum for Critical Communications could bring Broadband services over the 27 Member States of Europe more quickly.

Satellite networks can provide limited capacity on a nationwide (land and sea) basis from day one. Additional capacity can then be added as the terrestrial networks are rolled out. Satellite networks are less vulnerable to threat from physical terrorism or natural disasters.

The S-band regulatory situation is not standardised across the 27 EU Member States and the situation regarding the rest of the world is not clear. It should be noted that the solution described above is currently a proprietary solution.

The current satellite system is limited in capacity and resilience and is unable to meet the entire demands of the European Critical Communications sector immediately.

In addition to the proprietary solution described above, it is possible to use satellite services for backhauling of an ad-hoc LTE network. Today there are already mobile TETRA base stations that can be connected to a control room though a satellite link. Such systems may also be of value for remote operation of LTE systems. Issues regarding the use of common terminals with these services will need to be resolved.

Summary

There is no doubt that Mobile Broadband services are likely to bring significant benefits for many users of Critical Communications, enabling faster and more effective responses as well as efficiency savings for many organisations. Commercial broadband networks are already operational in many countries and roll out is accelerating as new spectrum is made available.

Commercial networks are already playing a role in many Critical Communications solutions and will continue to do so. They will enable users to experience the benefits of Broadband in a relatively short time.

[4] See NPSTC article:
http://www.npstc.org/download.jsp?tableId=37&column=217&id=2712&file=Why_Cant_PS_Just_Use_Cell_Phones_NPSTC_130415_orig.pdf

Work is on-going with the standards makers ETSI[5] and 3GPP[6] to develop the functionality that is already accepted as the norm by many Mission Critical and Business Critical organisations. It is, as yet, unclear as to when these services will become readily available. Mission Critical group based voice over LTE and communications outside of coverage of the infrastructure are particularly important issues whose solutions are still being developed.

The options described above are only high level descriptions and there will be many other possible variations on these basic concepts. However, it is hoped that this document will stimulate thought on how Mission Critical Mobile Broadband can best be deployed in each particular circumstance.

[5] ETSI - European Telecommunications Standards Institute is the Standards organisation responsible for the creation of GSM and TETRA

[6] 3GPP – 3rd Generation Partnership Project is the global Standards organisation responsible for the 3G and LTE standards.

Background

The Need

The CCBG Mobile Broadband Strategic Case documents will describe the need for Mission Critical Broadband and it is therefore not appropriate to go into the detail here. However, for those that are reading this document in isolation, a brief summary is given below.

Mission Critical Users

Users whose daily activities are fundamental to the health, safety and wellbeing of the citizens of this world and who depend on efficient mobile communications to carry out their job can be classed as Critical Communications users. Some of the most obvious examples are in the field of Public Safety and Critical Infrastructure services such as:

- Public Safety
  - Police
  - Civil Protection
  - Fire and Rescue services
  - Ambulance
- Utilities
  - Gas
  - Electricity
  - Water
- Transport
  - Buses and Trams
  - Trains and Metro
  - Ports and Airports

The above list includes some of the most obvious examples, but there are many other organisations for whom high availability, group based communications are of critical importance, often involving the safety of life.

Public Safety

Society is changing fast, and the way in which people communicate is changing even faster. These days many people organise themselves with social media applications such as Facebook and Twitter, and use these media as a matter of course, uploading images of situations at the click of a button. Tablets and smartphones with 3G, 4G or Wi-Fi connections make it possible for all of us to get information wherever we are and whenever we want, especially when mobile. Police officers, fire fighters and paramedics can take advantage of this wealth of up to date information to tailor their responses and make efficient use of resources. As society is changing, the work of these blue light organisations will change.

For example, streaming video from the scene of major incidents to a central control room will enable commanders to quickly determine how best to respond, thereby saving precious minutes in deploying resources to deal with a situation. Providing selected video clips to officers at the scene will provide them with better information on how to deal with a particular situation. Tracking of

human and vehicular resources is valuable in many situations and the ability to pass medical telemetry can be a lifesaver.

For 'business as usual' operation, access to back office systems from the street will enable staff to complete incident reports, access person, premises and vehicle databases, etc., and interact with the public via social media. This direct access to information systems will result in a higher degree of citizen engagement and increase the efficient use of staff.

Utilities

It can be argued that Electricity and Water are the two most vital commodities for the welfare of the citizen. Without water, humans can only survive a short time and without electricity many of the services that we take for granted quickly become unavailable – especially water. Gas, too, is a vital source of energy; powering many of our electricity generating stations.

The advent of smart meters and smart grids, along with the rapidly increasing diversity of local electricity generation, is creating huge challenges for electricity generators and distributors who carry the responsibility of maintaining a safe and coherent electricity supply. High speed, low latency monitoring and control are essential to achieving this goal. High quality - high availability data communications are needed to keep pace with this fast changing environment.

Transport

Transport is vital in today's world of highly mobile citizens. Fast and efficient transport is necessary in order to deal with the congestion caused by increasing traffic volumes. Obtaining up to date information on the location of buses and trains enables passengers to be informed of waiting time whilst supervisory staff can allocate additional capacity where necessary. Safety of the staff and the public is taking on an increasing level of importance. Real-time video from buses and trains enhances public safety and security and ensures that emergencies can be dealt with quickly and effectively. In the rail sector, a replacement for GSM-R will need to be found at some point in the future. Applications such as train control, line side signalling and other, increasingly complex applications will be required.

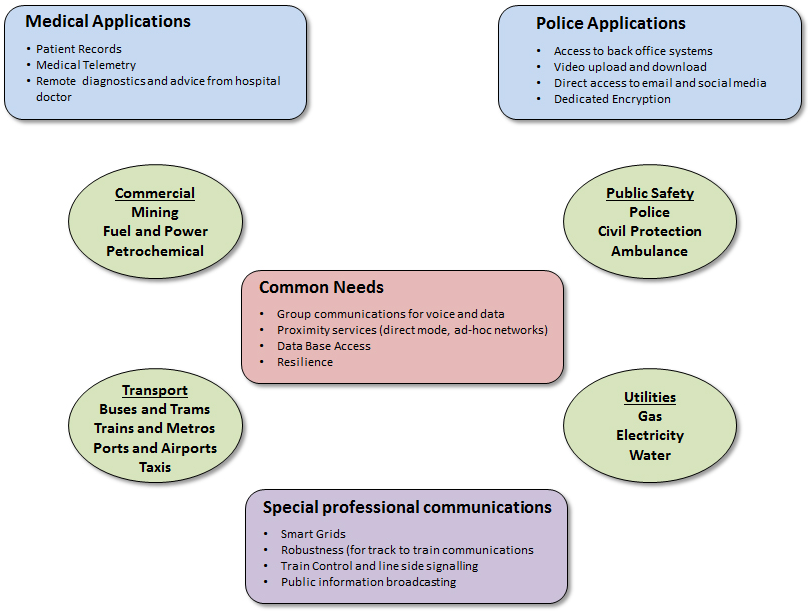
Ports and airports need fast and reliable communications in order to deal with the rapid turnaround of aircraft and ships, as well ensuring operations are conducted in a safe and secure manner. Accurate and timely information flows are essential to keeping transport moving, whilst ensuring that passengers are kept informed of delays or revised schedules.

Others

Customs and Excise, Coast and Border Guards, Military and Paramilitary, as well as Governments and their Administrations, are users of Critical Communications. In the commercial sector, Mining, Fuel and Petrochemical, Manufacturing and other forms of industry need group based resilient communications and all of these sectors are likely to take advantage of Broadband services.

Many of the Public Safety agencies are themselves dependent on other Critical National Infrastructures. Electricity is crucial to the provision of their services, as are water and transportation. There are significant interdependencies between all of these user groups.

Mission critical users have common needs and specific needs as showed below.



User Needs 1

Developments in progress

It is interesting to note that there are already many projects around the world where mobile broadband services are being implemented for Mission Critical users. Examples include:

- The State of Qatar which has already implemented a broadband network based on LTE for the Ministry of Interior. It is now fully operational and providing data services to the Security Departments.
- In the US the Obama administration has allocated 2 x 10MHz of spectrum and US$7 billion to stimulate the roll out of a Public Safety broadband network. This will initially support data services with voice being added later.
- In the UK the Home Office is developing a project to provide a Public Safety service based on LTE.

These projects demonstrate the importance of LTE as a basis for future Mission Critical data services and may also point the way for voice services in the longer term.

Spectrum

Several of the options described in this document rely on having the necessary spectrum in which they can be deployed. In these implementation models, spectrum and its availability are therefore key issues that will need to be considered.

In North America a block of 700MHz spectrum has been allocated for the creation of a Public Safety Broadband network known as FirstNet. In Australia and parts of the Middle East spectrum has also been allocated for Public Safety Broadband services. However, in Europe and other regions there is currently no allocation of spectrum for any form of private LTE networks.

The European Commission has, in its Radio Spectrum Policy Program, identified the need for PPDR[7] spectrum and CEPT[8] is investigating how spectrum can be made available. Even if a block was to be identified, it will be many years before such spectrum will become usable by Critical Communications users in Europe. The spectrum situation outside of Europe is variable, with some countries having already identified suitable spectrum. Any organisation that is planning to adopt LTE for data and/or voice will, therefore, have a different set of options available depending on when those services are required and in which geographic region they are located.

Timing Issues

The ability to provide mobile broadband solutions is heavily dependent on when these services are required and when they might be available. At the time of writing the LTE standard does not include group working or Direct Mode (device to device without infrastructure) capability. Even person to person voice over LTE is not yet fully standardised. Work is on-going in 3GPP to add additional core functionality to the LTE standard that will enable Group Call and Direct Mode. It is planned that this functionality will be included in Release 12 of the standard although some functionality may be delayed until Release 13. This release is unlikely to be complete before 2015.

Broadband services without Mission Critical capabilities can still be valuable to many organisations providing the limitations are understood by the end users. Commercial operators are likely to be able to offer such capability earlier than other implementation options.

As discussed above, the availability of spectrum will also have an impact on the ability to deploy mobile Broadband services if the 'dedicated commercial', 'owned and operated' or 'combination' models are employed. Spectrum in Europe is being sought through the European Commission and ITU World Radio Conference in 2015. See the TCCA Strategic Case document for more information.

Mission Critical Voice Services and LTE

Right from the first inception of commercial cellular networks, the primary requirement was to provide person to person voice calls, either mobile to fixed telephones, or mobile to mobile. This philosophy has carried on from the original analogue cellular systems through to GSM, 3G and now 4G. Over time the amount of data traffic has increased immeasurably but the person to person principle remains.

The Emergency Services, Critical National Infrastructure (CNI) industries and other business critical users frequently work in groups and therefore need to communicate in groups. As a result, Private Land Mobile Radio systems have been developed based on group communications as a primary function along with fleet management (grouping of subscribers) and Control Room functionality.

[7] PPDR is defined as Public Protection and Disaster Relief and includes Public Safety and other disaster relief organisations

[8] The European Conference of Postal and Telecommunications Administrations (CEPT) was established on June 26, 1959, as a coordinating body for European state telecommunications and postal organizations. Through its sister organisation 'Electronic Communications Committee' ECC, policies on radio telecommunications are formulated.

Imagine, for example, the chief of security at a football stadium wishing to inform all staff of a missing child and needing to communicate a description, perhaps with a photograph, to several hundred staff simultaneously. PMR systems are designed with this functionality at their core. If the stadium was only equipped with mobile phones it would take several hundred phone calls to pass that information to all staff. A situation that is clearly not viable.

The TCCA is working closely with the US National Institute of Standards and Technology (NIST), several Public Safety agencies and others to drive the development of additional functionality into the LTE standard. This additional functionality will provide group calling and also Direct Mode Operation (DMO) which enables calls to be made whilst out of the coverage of the infrastructure.

At the time of writing, 3GPP have accepted two Work Items for possible standardisation within the 3GPP working groups that will cover the Direct Mode Operation and Group Call functions[9]. It is hoped that these pieces of functionality will appear in Release 12 of the LTE standard which is currently scheduled for completion mid 2014 although some functionality may be delayed until Release 13 resulting in a delay of approximately 18 months. If these two items are successfully standardised then industry will need to incorporate these into future product releases. The current view is that this functionality could become available in products from circa 2016/17 onwards. To replicate TETRA or P25 functionality will require additional standardisation which is likely to be in the form of an "application layer" that will run over LTE's core services. This functionality is being standardised by ETSI.

ETSI is investigating what additional standardisation is necessary on top of the core LTE functionality to provide the more complex functionality normally associated with Public Safety and other Mission Critical systems. These might include:

- push to talk
- fast call setup
- emergency call
- group management and fleet management
- late entry (to a group call already in progress)
- area selection – a group call based on the location of individual subscribers
- call authorised by dispatcher – the ability of a central dispatcher to control who can talk and when (control room functionality)
- dynamic groups
- encryption
- etc.

As yet there are no timescales for the availability of such functionality

Voice services

The initial commercial driver for introducing LTE systems for most MNOs is to be able to deal with the rapid increase in data traffic resulting from smartphones, tablet PCs and computer dongles. LTE

[9] The particular WIDs (Work Item Descriptions) accepted by 3GPP are Proximity Services (ProSe) for Direct Mode and Group System Enablers (GCSE)

may also be used in rural areas to make up for the lack of broadband provided over traditional landline telephone circuits. The focus is therefore on data rather than voice. In the early implementations, it is expected that LTE data services will run in parallel to existing GSM and 3G voice services.

In the future it is likely that MNOs will wish to consolidate voice and data traffic onto a single network and work is going on to establish a common standard for voice over LTE.

In order to satisfy Public Safety needs for Mission Critical voice, it will be necessary for group services and Voice over LTE (especially group based voice over LTE) to be fully standardised. Currently it is early in the development cycle for this capability, especially when considering the additional functionality currently being looked at within ETSI.

The Implications

The level of uncertainty over the availability of voice functionality may cause users to concentrate firstly on utilising broadband data services and to enjoy the benefits of mobile access to remote databases, video and image transmission, mobile applications and others. When that capability has been developed and the coverage, resilience and service level agreements have been established, then it may be time to consider implementing voices services, once the standardisation and product development is complete.

It should be remembered that, for most critical communications users, voice services are considered to be the core Mission Critical function, given that users will often fall back to voice communications if all else fails. The loss of a data capability may be acceptable for limited periods in today's world, but the loss of a voice system is catastrophic.

In some cases it may be costly to utilise two separate networks for voice and data and there will be an incentive to incorporate voice services on to the LTE network once the Mission Critical functionality becomes available and assuming that the LTE network can provide the required coverage and resilience required by many Mission Critical users.

Implementation Options

This section is a review of the principle options for delivering Mission Critical Mobile Broadband. It does not make recommendations on the suitability of any particular service implementation but provides information to assist those who need to understand the possibilities and form their own conclusions about their suitability for a particular set of circumstances. It is feasible, or indeed likely, that a combination of the below options would provide the best solution, especially when balancing urgency and availability.

Take service from standard commercial networks

Introduction

In this delivery option the Mission Critical User makes an arrangement with one or more Mobile Network Operators (MNOs) for the provision of mobile broadband services.

The coverage and resilience of the standard commercial network will be the same as that which is provided for the commercial subscribers. The user may negotiate priority access to the network in certain situations.

The user will either take advantage of standard data devices, or purchase specialist compatible devices, to access the commercial network. This option may include the ability to operate on multiple networks using a roaming or multi SIM approach.

There are many different user groups who have Critical Communications requirements, including critical national infrastructure providers, commercial businesses such as petrochemical and power generation as well as Public Safety organisations, Governments and their administrations. Many of these will already have relationships with commercial Mobile Network Operators (MNOs) and, in the first instance, this solution may well be a 'natural' place to go for mobile communications access services even for users with critical requirements.

Description

Commercial mobile broadband networks already exist in a majority of countries. These networks use various 3G technologies, and over time, networks with higher dates rates and increased coverage will be rolled out.

There is a technology convergence towards 4G/LTE taking place, which will create significant economies of scale. Users can leverage the buying power of the Public Safety sector to pool the demand in one or more contracts and to execute long term service procurement with existing communication providers.

The Mission Critical user then takes service from the service provider, using that provider's normal commercial network, and to a service level agreement (SLA) which has been negotiated with the service provider. This may include:

- priority access in critical incidents
- a response time for network outages
- a target for coverage

- a target for latency

The service provider will negotiate the SLA based on commercial pressures. The fact that they have a standard commercial network, and that the Mission Critical user often represents a very small proportion on the subscriber base, means that the provider may not be prepared to offer a bespoke SLA, but offer the service on a 'best endeavours' basis. However, the user may find that relatively short term contracts enable greater competition and the best available prices.

Advantages

The key advantage to this option is that 3G and 4G data networks already exist. Agencies will be able to implement mobile broadband solutions early and explore some of the possibilities that broadband data offers without significant upfront investment.

This option can also be a very cost effective solution, since there is no infrastructure Capex and, since the network is supporting many more commercial users than Mission Critical users, there are significant economies of scale.

Standard terminals can be used, with purchasers enjoying the benefits of scale accruing from a huge market for commercial cellular terminals and a highly competitive supplier base. Specialist terminals for specific applications are likely to become available in time.

There will almost certainly be competition for the user's business from multiple service providers. Data bundles with the commercial service provider can be negotiated.

With no infrastructure costs and cheaper commercial terminals being used, terminal refresh can be performed more frequently, which allows the user to maintain the latest technology curve, as networks move from 3G through HSPA and HSPA+ to 4G.

Whilst early implementations may be limited to basic services (i.e. no Direct Mode, no Group Call capability and no voice services) it may be possible to obtain new capabilities as and when 3GPP's Critical Communications specific features are released. Current estimates are that some of these features will become available from circa 2016 onwards.

Disadvantages

The main disadvantages are that the user has no control over the coverage, availability or resilience of the network. The network is a standard commercial network, which will be designed to meet commercial imperatives. This will often mean designing for premises coverage rather than geographic coverage, and not including resilience into the network architecture, except in the central core network. Many core elements of a commercial network, such as the Home Location Register, are not resilient, and many failures have occurred resulting in loss of service for several hours at a time. Sites may not be protected against power failure, which makes the network totally unsuitable for a power utility and generally unsuitable for many other critical users.

There may be a dependency on one network which, if the network fails, would result in all Mission Critical users losing service. If the user decides to take service from two or more operators, care has to be taken to ensure that they do not share common elements of the radio access network, which is increasingly common, and may not be obvious to the user.

If service is taken from multiple networks with independent infrastructures, it may be necessary to use more than one SIM, as roaming within the home country is usually not allowed (although is becoming available for M2M applications). This can be overcome by making an agreement with an operator from a different country but then roaming charges may be an issue. The MVNO approach described later may be a better option.

The user will have to accept the network provider's standard functionality, which will not, in the short to medium term, provide key Critical Communications features. Depending on the criticality of the users' applications, this may not be an issue, but may limit the services that the network can be used for. For Public Safety this will almost certainly mean the provision of a parallel network for voice and critical data.

Once the standards work is complete, and Critical Communications key features are included in the LTE standard, there is no guarantee that such features will be implemented on individual networks. The user will be in the hands of the network operator as to when it is commercially viable to introduce these features into the existing network, and it is possible that some or all are not introduced at all.

If Mission Critical features become important then users will need to build their provision into the service contract. It is likely that only some elements of the Critical Communications key features list will be incorporated into the LTE standard, and that an application outside of the LTE network will be required to carry this functionality. This is currently being worked on by ETSI. The user will need to procure this application and arrange for it to be interfaced to the commercial network.

If the user chooses to enter into a long term contract due to commercial pressures, then they will be in a difficult position to engage in further negotiations, and have little control of the service provider in the event of, for example, ownership changes to a foreign company or competitor.

Unless the user has been able to negotiate guaranteed capacity on the network there is a danger that access will become restricted, or lost altogether, during times of peak demand. Experience shows that such peaks often occur during major incidents when Critical Communications users often need the service most.

Operate as a Mobile Virtual Network Operator (MVNO)

Introduction

MVNO stands for Mobile Virtual Network Operator, and is a business model where the MVNO makes a contract with a commercial cellular Mobile Network Operator (MNO) to "buy" access to the MNO's network for its own customers.

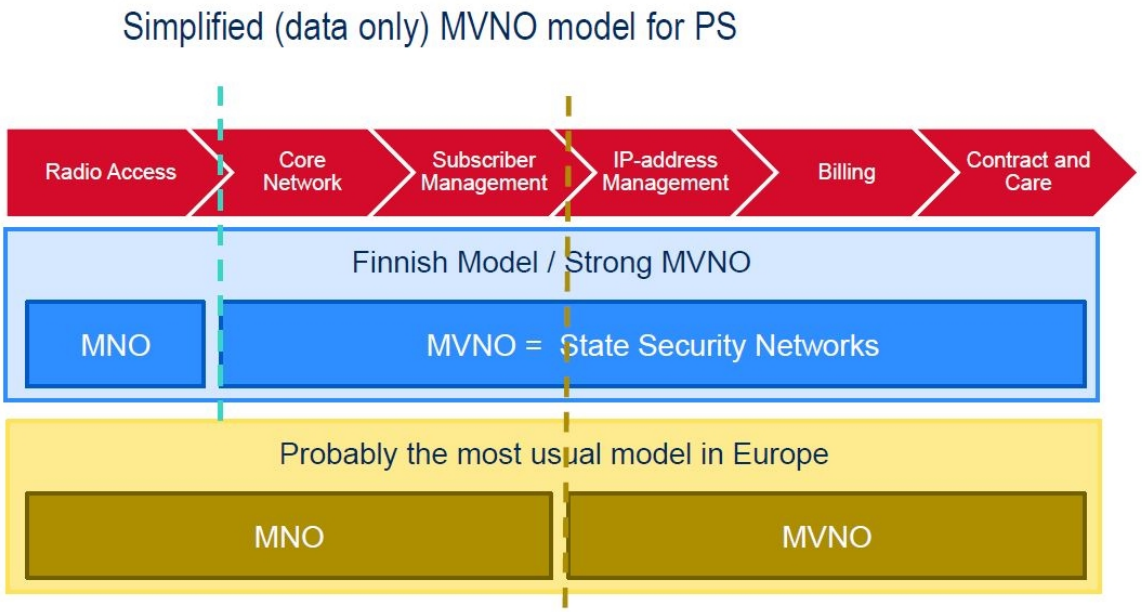
MVNO models have existed for more than 10 years in the commercial cellular environment and the principles are therefore already well established. Cellular operators will be aware of the mechanisms for enabling third parties to set up as a MVNO. However, there are many different ways of implementing the MVNO model depending on how far the MVNO wants to control its services and how much control an MNO is willing to offer.

The success of the business model is dependent on creating a win-win situation between the MVNO and the MNO, where the MVNO has more knowledge than the MNO of a specific market segment and which the MNO may not wish to develop itself. This may be due to particular market circumstances and/or difficulties in penetrating that market segment.

The market segment of "Critical Communications" might be seen by a MNO as a small, but very demanding, market in comparison to the typical large consumer market that it is normally addressing. This is where the MVNO can fill the gap and bring value.

In the case of Critical Communications, the goal of the MVNO is to leverage the existing commercial mobile broadband radio infrastructure to create and operate dedicated services for the critical users, with short time to market and relatively low Capex.

The diagram below shows how a Critical Communications MVNO model may differ from a typical commercial MVNO arrangement.



Description

The MVNO has to have deep expertise in the relevant mobile communication technologies and a thorough understanding of the critical user requirements in order to make the best use of the existing commercial cellular radio infrastructures if it is to create and operate services dedicated to critical users.

The MVNO has to negotiate special contractual arrangements with the MNO and a detailed Service Level Agreement (SLA) to reach its objectives. In order to spread the risk of network failure and exceptional traffic conditions as well as improving coverage, it may be advantageous to negotiate capacity with two or more MNOs.

Those dedicated services can deliver added value including better availability, security, quality control, and better customer care than can be delivered by the commercial MNOs individually.

Better availability can be achieved by allowing roaming to any of the national MNOs. This also results in achieving the best coverage possible and as well as improved resilience, provided the infrastructures are not shared. Availability is also increased by granting higher access priority on to the commercial infrastructures based on special agreements with the MNO's. Security and confidentiality of the data-flows can be managed by the MVNO for the benefit of its users.

The MVNO stands between the users organisation(s) and the MNO's and it manages all the services for the users, such as provisioning, monitoring, managing all operational processes including incident, problem, change, configuration, and release management that are needed to control the quality of the services.

The MVNO will also manage the funding and financial aspects of the project.

Advantages

With the MVNO pooling all of the Critical Communications users together, the MVNO can drive the commercial operators and seek to make them more creative in delivering dedicated services for the Users.

For existing PMR operators (TETRA, Tetrapol, etc.) the MVNO model provides a step towards an eventual dedicated broadband network in the future whilst enabling the operator and users to better understand the benefits and delivery of mobile broadband.

In the longer term, the MVNO can be seen as the first part of a hybrid solution described later in this document.

The MVNO model can be used as a tool box that will help to adapt services to the evolving requirements of the user's mobile data applications. Critical Communications users are now at the early stage of a new era regarding mobile data applications and they will face growing and changing expectations towards the mobile data services.

The MVNO model is very efficient especially looking for a "shared" network/solution between different critical users organisations, as it enables them to reach an economy of scale through a common approach rather than each organisation setting up its own MVNO with the MNO's.

A shared solution, through an MVNO, will also create an environment that will facilitate the exchange of information between user organisations when needed.

Disadvantages

As with standard commercial networks the MVNO solution will only provide service where the operators have installed coverage.

Similarly, network resilience levels will only be that which is considered necessary by a commercial organisation. Experience shows that the network resilience of many commercial operators is limited, with many reported instances of significant network outages from a range of operators. Utilising several commercial networks will have a positive impact on service availability providing they have separate infrastructures, however experience shows that, in times of crisis, commercial networks are more likely to fail than networks built for critical communications use.

The degree of importance is, of course, dependent on the criticality of the service being taken. A data-only service is often considered non critical whereas voice service is absolutely “Mission Critical”. This distinction may become less apparent in the future with many users expecting that a high proportion of mobile data applications will become Mission Critical in the not too distant future.

At this stage, Mission Critical functionality (e.g. group working and communication out of network coverage) is not yet standardised. It is unclear how willing commercial operators will be to add this functionality later especially as Critical Communications Users are likely to represent only a small proportion of the operator’s overall business.

At times of major incident, commercial networks tend to become overloaded. Some operators have agreed to provide priority access to the network when required. There is little experience so far of how successful this priority access will be when the network is under stress.

Take service from Commercially Owned Dedicated Network

Introduction

In this solution the Mission Critical User contracts with a commercial organisation to build and operate a dedicated network. The network may be dedicated to one particular user, or may be dedicated to Critical Communications use, but is more likely to provide service to multiple Mission Critical users.

Since the network is dedicated to Critical Communications use it can be built with suitable coverage and availability criteria, and the users can demand some control of the network and the operator. It can be specified to have Critical Communications key functionality, or, if this is not available within the standard at network build time, the network operator can be obliged to provide it when it is available.

Description

A commercial operator deploys a mobile broadband network, and then offers service to Critical Communications users.

This model is currently in use for some narrowband and wideband public safety network deployments globally. Key requirements to take advantage of such a model are:

- There are resources available to deploy a dedicated network. These include funding, spectrum rights, etc.
- There is sufficient pooling of demand to justify the creation of a dedicated network for commercial partners. (Typical sharers may include Police, Fire, Ambulance, Customs, Border Guards, Utilities, Transport companies etc.)
- The need for differentiated features and service levels

To implement such an approach, a public procurement will need to take place for a significant share of the Critical Communications market for the nation. A single commercial company or a consortium of investors/industrial partners would need to invest in a dedicated network development. The consortium could include existing MNO's or existing TETRA/Tetrapol network operators, but could also be established by a completely independent company.

The model requires that the company or consortium invests in technology deployment on the basis that it becomes the sole operator for the provision of mobile broadband communications to the Mission Critical sector. In order for the business model to be viable it is likely that the network would need to be amortised over at least a 15 year period.

Advantages

The significant advantage of this solution is that the Mission Critical users are the only people using the network. Control can be exercised as to priorities of access, and there are no commercial users to take capacity during an incident. Since the network is being built for Mission Critical users, their requirements in terms of coverage, availability and resilience can form part of the contract.

During the procurement phase the potential supplier will still be under commercial pressures and the user will be able to negotiate the design of the network. This will enable the user to tailor the

design to their requirements compared to having to accept the design of a commercial network. The contract between the network operator and the users can define the obligations of the operator, including specified service levels and a functionality roadmap.

The key Critical Communications functionality requirement, if not available on Day 1, can be built into the contractual arrangements; the network can be designed to support the upgrade, and without commercial users to consider, the upgrade can be carried out more effectively and at an earlier time.

The Critical Communications sector can pool its buying power into a single procurement, thereby ensuring sufficient demand to obtain best pricing for the procurement of mobile broadband communications services.

The Critical Communications sector is in the driving seat to produce its Requirement Specifications and to define its requirement and adapt its service roadmap over time.

Depending on the consortium participants and contracts, essential (and expensive) components of the LTE infrastructure can be shared with commercial MNO networks (sites, masts, power supply, backhaul network, etc.) [See also Chapter on "hybrid" approach] It is also possible for the user organisations to lease or share their own existing network elements to the network operator.

Disadvantages

In order to pursue this option a commercial operator will need to be convinced that there is a viable business case and that a return can be made on an investment lasting probably a minimum of 15 years. It follows that the Critical Communications Users (or national Government) will need to make a long term commitment for the business case to be viable.

Availability of spectrum is a significant issue. It is already clear that spectrum for mobile broadband is under heavy demand and there is limited support from regulators to allocate sufficient spectrum solely to PPDR [10] and other Critical Communications users. Whilst the Critical Communications community, supported by the TCCA, is lobbying hard for the necessary sub 1GHz spectrum there is still uncertainty over its allocation.

It is possible that individual countries may find unique spectrum allocations where such services could be deployed. However, if a non-standard band is utilised then costs for specialised infrastructure may be high and a competitive ecosystem of terminal equipment may not be available. It is therefore important to have at least a regional, if not a global, harmonisation of spectrum use.

Timescales for implementation may also be an issue. The procurement process and network build out will typically take 3/5 years to deliver the first service to users, thereby delaying the start of broadband services for the users of that network.

[10] Public Protection and Disaster Relief (PPDR) is a term that encompasses the traditional Public Safety organisations and also major incident rescue services. First mentioned in ITU Report ITU-R M.2033, 2003, "Radio communication objectives and requirements for public protection and disaster relief (PPDR)"

Build Own and Operate a Dedicated Network

Introduction

In this solution the Mission Critical User builds and operates a dedicated Mobile Broadband network. The network may be dedicated to one particular user, but for financial as well as operational reasons, will probably be dedicated to Critical Communications use, and be available to multiple Mission Critical users (such as Police, Fire, Ambulance).

Since the network is dedicated to Critical Communications use it can be built with suitable coverage and availability criteria, and the users will have absolute control of the network. It will be specified to have Critical Communications key functionality, or if this is not available within the standard at network build time, the network supplier can be contracted to provide it as an upgrade when it is available.

Description

This is the most common model of deployment for narrow band and wideband Public Safety networks in most European countries. The State (the Government) directly or via a controlled entity procures equipment, deploys and operates a closed network dedicated to the Critical Communications users for a period of up to 15 years or more.

In many countries the State creates a 'pseudo independent' operator, often state owned, in order to take responsibility for the build, management and financing of the network. It assumes that the State is prepared to dedicate resources (particularly spectrum and funding) to enable the project to go ahead.

In Europe, the telecom regulators of Member States have dedicated a portion of narrow band spectrum for Public Safety users on a harmonised basis across Europe.[11] This makes it possible to achieve cross border working and allows industry to develop equipment to a common frequency band, thereby benefitting from economies of scale. A similar arrangement would be needed to provide Mobile Broadband services.

However, due to the high cost of developing chipsets and radio equipment it is important that harmonisation takes place on as much of a world-wide basis as possible.

Advantages

The primary advantage for this option is that the Critical Communications users and national Government have full control over the procurement process, the network procured and the operating assets.

The network can provide a total match to the Critical Communications key requirements, either at Day 1 or by way of an upgrade, It has the ability to provide 'best fit' technology for blue light and other Critical Communications users.

[11] The NATO band 380-400MHz was made available for Public Safety use throughout Europe and this band has been adopted in many other countries of the world. In some countries 410-430MHz was also allocated for non Public Safety use.

The users will have complete control over the network management, thus ensuring that, through the use of priorities, the capacity on the network can be managed and tailored to changing circumstances. In times of crisis or major incident the operator can ensure that those who need the service will not be blocked by overload from the general public.

If harmonised spectrum is available, cross border agreements between Mission Critical Users can be negotiated, without involving third party operators, and encryption codes can be shared.

Disadvantages

At the time of writing, the lack of certainty over spectrum brings its own challenges when considering this option. Significant effort is being put into addressing this problem. Even so, harmonised spectrum is unlikely to be allocated much before 2015. It will take several more years before such spectrum can be cleared and made available for use.

In today's economic climate the lack of funding for dedicated private networks is likely to be the biggest hurdle to overcome. However, the advantages of providing users with guaranteed capacity and coverage that is not restricted to areas that generate maximum income, as is the case with commercial cellular systems, cannot be ignored. If operators are considering using a mobile broadband network for voice services these benefits become even more significant.

Note

In the light of the above observations it becomes likely that alternative options will need to be employed in order to provide broadband services whilst funding and spectrum issues are resolved. This clearly complicates the situation as further procurement processes will be involved. However, it could be argued that the use of alternative approaches as an interim measure could enable users to gain experience in the use of mobile broadband data and assist in the development of future plans.

A Combination Approach

Introduction

In looking at the available implementation options, a user/operator may conclude that none of the above options adequately meets the need in their particular circumstances. However, a combination or hybrid approach may provide the best compromise. As described above and, as an example, the availability of dedicated systems may be too far in the future. An alternative solution for the most important geographical areas may be an acceptable starting point.

Description

There are two different reasons for considering a combination approach. One is to solve the timing issues, where dedicated networks are not available early enough and the second is to address coverage and functionality issues.

As already described, with dedicated networks potentially further away in time due to spectrum and funding issues, it may be realistic to utilise commercial cellular operators or an MVNO approach in the early years and then migrate to a dedicated network once this becomes a viable option.

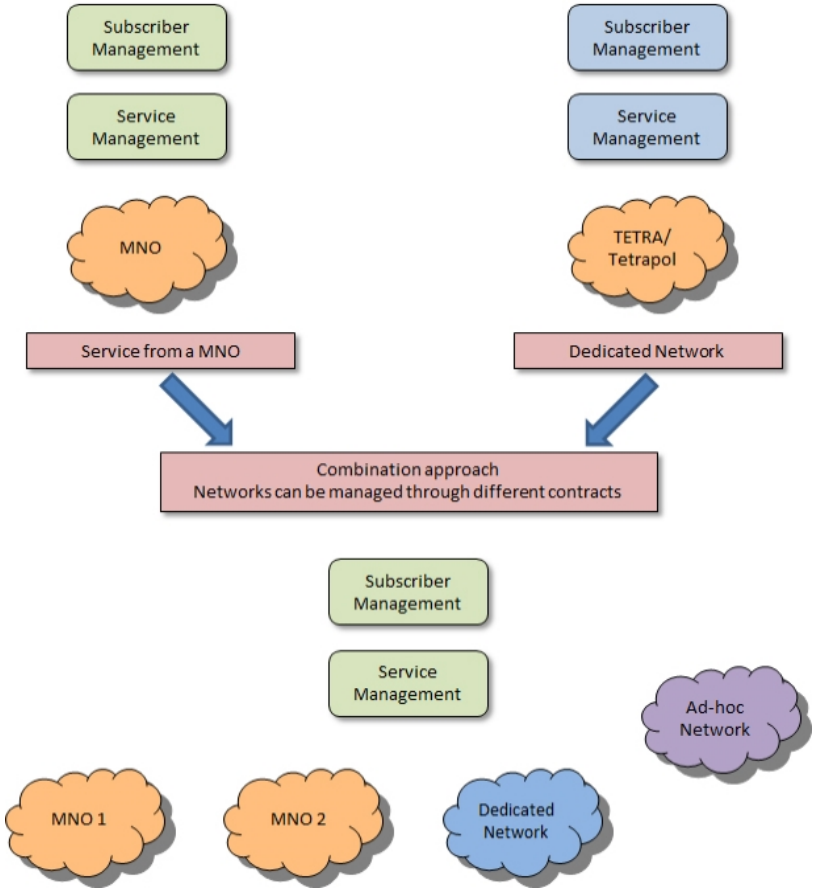
Alternatively it may be that dedicated networks are unaffordable and that a commercial operator or MVNO approach will provide service to a percentage of the geographic coverage required. Where there are holes in the coverage then the Critical Communications user may decide to build additional coverage to fill in the gaps. Roaming between private and public systems can be achieved with appropriate contractual relationships.

In addition to using private systems to solve coverage gaps it may also be possible to overlay private networks on top of commercial networks in order to obtain some guaranteed capacity should the commercially provided networks become overloaded. Some sharing of infrastructure may reduce the cost of such an arrangement.

As Critical Communications specific functionality becomes available it may be viable for a user to have the additional functionality from a private network whilst falling back to the commercial network for more conventional usage. For example, group calling functionality may only be available from a private overlay network whilst Internet, email and database lookup functions could be handled over a commercial network.

As described above, there are likely to be coverage, capacity, resilience and/or functionality limitations from standard commercial offerings. It may be more cost effective to come to an arrangement with an operator to add coverage, capacity, resilience or functionality at the user's expense rather than invest in a fully dedicated network. Such an arrangement would, however, result in the network operator having a competitive advantage over other operators. It is unclear whether such a subsidy would breach local competition laws.

Clearly it will be necessary for a user to prioritise their requirements before determining which combination of available options best meets their needs.



Combination Approach 1

Advantages

A combination approach firstly addresses the problem that preferred solutions may not be available for some time to come, whether it is through spectrum, functionality or funding issues. In addition, the various combinations described above provide users with considerable flexibility. In particular they will be able to experiment with the use of broadband mobile data and determine which applications or pieces of functionality are the most important and that need to be addressed in a later solution.

A combination approach enables agencies to benefit from some broadband services whilst waiting for the full Critical Communications functionality to become available.

In the current economic climate, funding of new networks is extremely difficult. A combination approach enables users to delay, or at least minimise, capital expenditure until later years whilst building up evidence of the benefits that such services provide.

Disadvantages

Any approach that is based on multiple solutions will inevitably require more resources to manage and greater expertise to bring these solutions together.

With a solution involving multiple elements it will be more difficult to negotiate value for money contracts with potential suppliers, thus resulting in increased costs in the long term. In some cases it may not be possible at all if the commercial operators cannot develop a viable business case.

If temporary solutions are implemented for a period of time before switching to a second solution, end users could become confused and additional training may be required.

Multiple solutions provided by different suppliers may make it more difficult to organise cross-border and multi-agency solutions.

RAN Sharing

RAN (Radio Access Network) sharing is somewhat outside the scope of this document as it involves two or more operators sharing a network at a more detailed level than, for example, an MVNO. RAN sharing is a capability that is being built into the 3GPP standards and is due to become available in Release 12 of the LTE standard. It is mentioned here as it might be of potential interest to some users who may wish to utilise an existing network in some regions and build their own network elsewhere.

Detailed information on RAN sharing can be found within the 3GPP standards documents. The following information is extracted from 3GPP TR 22.852 V12.0.0 (2013-06)[12]

The arrangements for network sharing between the involved entities can vary widely, being influenced by a number of factors including business, technical, network deployment and regulatory conditions. Within all of this variation, there is a set of common roles centred around connecting network facilities between the parties participating in a network sharing agreement. This section presents these common roles to aid in understanding the entities described in the use cases.

Hosting RAN Provider

The Hosting RAN Provider is identified as sharing a hosting RAN with one or more Participating Operators. The characteristics of the Hosting RAN Provider include:

- *Has primary operational access to particular licensed spectrum which is part of the network sharing arrangement.*

Note: The Hosting RAN Provider does not necessarily own licensed spectrum but has agreement to operate in that spectrum.

- *Has deployed a RAN in a specific geographic region covered under the network sharing arrangement*
- *Operates the RAN identified in the previous two items.*
- *Provides facilities allowing Participating Operators to share the RAN covered under the network sharing arrangement*

Within the concept of a Hosting RAN Provider, other entities can be involved such as outsourcing, joint ventures, or leasing agreements such as for operating, owning the RAN infrastructure or managing the sharing agreements.

Participating Operator

[12] 3GPP TR 22.852 V12.0.0 (2013-06)
Technical Specification Group Services and System Aspects;
Study on Radio Access Network (RAN) sharing enhancements
(Release 12)

The Participating Operator is identified as using shared RAN facilities provided by a Hosting RAN Provider, possibly alongside other Participating Operators. The characteristics of the Participating Operator include:

- *Uses a portion of the particular shared licensed spectrum to provide communication services under its own control to its own subscribers.*
- *Uses a portion of the shared RAN in the specific geographic region covered under the network sharing arrangement.*
- *Within the concept of a Participating Operator, other entities can be involved such as outsourcing, joint ventures, or leasing agreements such as for operating or owning the service infrastructure.*

Operators with multiple roles

Operators can take on multiple roles at the same time depending on business needs. For the purposes of this TR, each specific network set (spectrum-region-RAN) can be considered independently and combined with other network sets in various combinations.
Examples include:

- *An operator has its own spectrum which he does not share and additionally uses the shared RAN in the same region (Participating Operator) provided by Hosting RAN Provider.*
- *Two operators set up a joint venture to build and operate a shared network. The two operators are both Participating Operators and the joint venture is a Hosting RAN Provider.*
- *Two operators A & B, divide a region covered by a joint spectrum license and each build and operate the RAN in their portion of the region. In the region covered by operator A's RAN, operator A is the Hosting RAN Provider and at the same time Participating operator while operator B is only Participating Operator. In the region covered by operator B's RAN, operators A and B are the Participating Operators and operator B is the Hosting RAN Provider.*

As can be seen from the above, opportunities exist, for example, for a public safety network operator to build a radio network in areas not of interest to an existing MNO but to share each other's networks through a formal agreement. This may seem to be similar to a roaming agreement. However, the distinction between roaming and RAN sharing is:

- when roaming, the subscriber uses the Visited Network when outside of the Home Network geographic coverage and within the Visited Network's geographic coverage
- in a RAN sharing arrangement, all of the participants (Hosting RAN Provider and one or more Participating Operators) provide the same geographic coverage through the Hosting RAN.

For further information on RAN sharing please contact the TCCA Critical Communications Broadband group CCBGSec@TandCCA.com

Other Hybrid Approaches

Introduction

Within the previous approaches there are a number of hybrid approaches. These are illustrated in the following table

Description	Advantages	Disadvantages
Take service from standard commercial networks, but fund network enhancements on coverage and resilience	• Network can be engineered to meet some of the Critical Communications key requirements • Lower CAPEX and OPEX	• May be classified as State Aid • Forces a long term arrangement with one MNO • May need governmental investment in all MNO networks and lost investment if MNOs merge
Take service from Commercially Owned Dedicated Network, but allow operator to sell excess capacity to commercial users	• Economies of scale improve for the network operator, with more viable business case • Easier for Public Safety users to justify spectrum • Attractive high quality network for professional commercial users with premium rate possibility • No CAPEX and Lower OPEX	• Some loss of control once the network has commercial users • Commercial users may be hesitant to move to network, if they know their service may be degraded during an incident • May be difficult to control if all resources are available for Critical Communications users
Build Own Dedicated Network, but outsource operation of the network	• Allow an external more focussed and capable organisation to operate and manage the network • Lower OPEX	• Need to form a commercial long term arrangement with a suitable operator • Operator will charge for service • Higher CAPEX
Build dedicated network but share network elements with commercial operators. i.e. share towers and backhaul but add own radio access network.	• Reduces CAPEX requirements • Eases planning and site building requirements • Reduces network management costs • Lower CAPEX and OPEX	• Increases reliance on commercial operator • Coverage may not be tailored to Critical Comms users' requirements • Network resilience may be compromised

FirstNet

Readers of this document may well be aware of the US Mission Critical Mobile Broadband initiative in the US that is now known as FirstNet.

As a result of a coordinated national campaign from Public Safety, the US Government allocated 2x10MHz of spectrum in the 700MHz band and 7 Billion US Dollars to stimulate the roll out of a nationwide Public Safety Broadband network. The Department of Homeland Security tasked the NTIA (National Telecommunications and Information Administration) with the responsibility of making this happen. The NTIA set up a new organisation to manage the process and this organisation is now known as FirstNet.

At the time of writing there is much uncertainty about how FirstNet intends to satisfy the user's needs, as their first priority seems to have been to concentrate on creating the FirstNet organisation and recruiting staff. Initial indications are that, rather than attempt to build a dedicated broadband nationwide network, FirstNet will act as a management organisation to oversee the development of contractual arrangements with commercial operators to provide service.

Prior to the establishment of FirstNet, a number of agencies obtained waivers from the FCC to use some of the allocated spectrum and started the process of building broadband networks of their own. This has caused something of a headache to FirstNet who needed to find a way of integrating these networks into a national plan. After initially withdrawing the licences, FirstNet have been negotiating with these agencies to include them in the overall network.

Another major uncertainty revolves around whether the FirstNet system is being planned to carry voice services or just data. The National Public Safety Telecommunications Council (NPSTC) issued a statement to its members suggesting that the availability of Mission Critical Voice over LTE is uncertain and not likely to be available for many years, if at all. NPSTC urged users to continue to maintain and invest in their existing Land Mobile Radio voice networks. (See footnote for a link to the NPSTC statements.[13])

As FirstNet continues to develop its plans, their experiences may well provide insight into some of the options available to users and Governments outside of the USA.

Due to the close geographical relations ship to the USA, Canada follows many of the US initiatives, especially in relation to spectrum planning. At this stage there is no indication that Canada will follow the FirstNet principle but may choose to do so if it becomes successful.

[13] http://www.npstc.org/download.jsp?tableId=37&column=217&id=2712&file=Why_Cant_PS_Just_Use_Cell_Phones_NPSTC_130415_orig.pdf

The Role of Satellite Services

Introduction

Satellite services are able to provide Public Safety users with communications over very wide areas and are therefore particularly well suited to locations hard to reach or justify with terrestrial networks. In May 2009, the European Commission granted two European satellite operators the right to operate 2 x 30.0 MHz (2170-2200 / 1980-2010) of mobile satellite service (MSS) spectrum using a complementary ground component (CGC) network . The use of this spectrum asset has been granted for a period of 18 years and covers the 27 Member States of the European Union.

The CGC network consists of a core terrestrial network that is to be operated in an integrated fashion with a satellite segment of the network.

This new network configuration combines the geographical coverage benefits of the satellite with the high throughput of terrestrial mobile communications networks.

Description

The MSS spectrum band as described above provides an option to the Public Safety sector to implement a “commercially owned dedicated network” approach relatively quickly. A terrestrial network can be deployed in areas where higher capacity is needed whilst rural areas can be covered by satellite services. Vehicle mounted access nodes provide a direct connection between the local radio access gateway and the satellite in order to provide the backhaul from the local radio access to the Network Operations Centre (NoC).

The MSS spectrum band is currently unencumbered and available across the entire 27 Member States although some regulatory approvals still need to be obtained. The satellite segment of the network was launched in 2009 and can support service launch for a portion of the EU Member States immediately. Additionally, the MSS spectrum band is set to become 3GPP compliant and hence can be deployed in Europe leveraging the economies of scale of the LTE ecosystem globally.

Outside of Europe, satellite services can still be utilised though appropriate spectrum agreements would need to be negotiated.

Advantages

With the issue of spectrum for Critical Communications users still uncertain, the development of a dedicated network using the MSS S-band spectrum for Critical Communications could bring Broadband services over the 27 Member States of Europe more quickly. The deployment of a dedicated network using the S-band spectrum can prove to be very cost effective as it requires the terrestrial network to cover only the areas that are hard to reach via satellite (natural canyons) or to cover hot zones (i.e. zones with high operational requirements such as city centres) with high throughput networks.

In areas where a terrestrial network is to be developed, the MSS S-band can be deployed using the physical layer of an existing 3G network thereby reducing the requirements for building new base stations and backhauling facilities.

Assuming that enough Critical Communications users pool their service requirements together and are willing to engage in a long term commitment, satellite operators are willing to pre-finance the deployment of 2.1 GHz networks (terrestrial and satellite segments) and to dedicate a significant portion of the network to the use of Public Safety users. 3GPP compliant technology can be available within 2 years.

Satellite networks can provide limited capacity on a nationwide (land and sea) basis from day one. Additional capacity can then be added as the terrestrial networks are rolled out.

Satellite networks are less vulnerable to physical acts of terrorism or natural disasters.

Disadvantages

The S-band regulatory situation is not standardised across the 27 EU Member States. The deployment of a pan-European solution in S-band would be aided by a common regulatory framework. The lack of such a framework may delay the availability of an appropriate licence to operate the convergent network in some European countries.

The satellite based technology to support the “service vehicle as an access node’ is a proprietary technology that still requires development and industrialised production. The availability of a mass production technology is likely to take 18 months.

The current satellite system is limited in capacity and could not meet the entire demands of the European Critical Communications sector immediately. The development of the market on a pan-European basis would require a new high performance satellite to be manufactured and launched. Projected timescales for the availability of a new satellite capable of supporting all 27 EU Member States is Q3/2016.

Scenarios need to be developed to satisfy Critical Communications users outside of Europe.

Satellite failure due to technical or natural disasters in orbit would be difficult to resolve.

Conclusions

There is no doubt that Mobile Broadband services are likely to bring significant benefits for many user of Critical Communications, enabling faster and more targeted responses as well as efficiency savings for many organisations. Commercial broadband networks are already operational in many countries and roll out is accelerating as new spectrum is made available.

Commercial networks undoubtedly have a role to play in many Critical Communications solutions and will enable users to experience the benefits in a relatively short time.

Work is on-going with the standards makers in 3GPP, ETSI and elsewhere to develop the functionality that is already accepted as the norm by many Mission Critical and Business Critical organisations. It is, as yet, unclear as to when these services will become readily available. Mission Critical group based voice over LTE is a particularly important issue that has yet to have firm plans drawn up to provide acceptable solutions.

The options described above are only top level descriptions and there will be many possible variations on these basic concepts but hopefully this document will stimulate debate on how Mission Critical Mobile Broadband can best be deployed in each particular circumstance.

For further information please see www.tandcca.com

Glossary

3GPP	3rd generation Partnership Project – the organisation responsible for the LTE standard
4G	4th Generation cellular radio technology
CAPEX	Capital Expenditure
CCBG	Critical Communications Broadband Group. A working group of the TETRA and Critical Communications Association
CEPT	European Conference of Postal and Telecommunications Administrations – a coordinating body for European state telecommunications
CGC	A Complementary Ground Component is a terrestrial infill system for a mobile satellite system that uses terrestrial base stations to provide connectivity in weak signal areas such as urban areas
CNI	Critical National Infrastructure typically includes the Utilities (Gas, Electricity and Water), Transportation (Rail and Metro, Buses and Trams, Ports and Airports) and other critical industries without whom society would quickly break down
DMO	Direct Mode Operation. A means of establishing communications between two radios without the intervention of a radio infrastructure
EC	European Commission
e-nodeB	e-nodeB (or ENB) is the radio base station and controller in an LTE network
ETSI	European Telecommunications Standards Institute
EUTC	European Utilities Telecom Council – an Association of Utility organisations in Europe similar to the UTC in the USA
e-UTRAN	e-UTRA is the air interface of 3GPP's Long Term Evolution (LTE) upgrade path for mobile networks. E-UTRAN is the radio access network based on that standard
EPC	Evolved Packet Core is the overall packet data handling system of a LTE network.
FCC	Federal Communications Commission – the US regulator
FirstNet	First Responder Network Authority (FirstNet)is an independent authority whose task is to provide emergency responders with the first high-speed, nationwide network dedicated to Public Safety in the USA
Group Call	A means of setting up a radio call to a large number of users simultaneously
HSPA	High Speed Packet Access is a 3G technology for delivering high speed data over a cellular telephone network
HSPA+	Evolved High-Speed Packet Access, is a technical standard for wireless, broadband telecommunication that provides increased data rates over HSPA
ITU	International Telecommunications Union – coordinates the shared global use of the radio spectrum
LMR	Land Mobile Radio is the US equivalent of PMR and also provides group based radio communications
LTE	Long Term Evolution – the latest standard for cellular communications. LTE provides higher data rates than 3G UMTS but is not quite a 4G technology
LTE-A	LTE Advanced – A further development of the LTE standard defining additional functionality including aggregation of separate frequency bands and the addition of voice services. LTE Advanced is considered a true 4G technology
M2M	Machine to Machine communications
MCMBB	Mission Critical Mobile Broadband
MNO	Mobile Network Operator – A commercial cellular network Operator

MSS	Mobile Satellite Service
MVNO	Mobile Virtual Network Operator
NIST	The US National Institute of Standards and Technology is a measurement standards laboratory, and is a non-regulatory agency of the United States Department of Commerce. NIST is currently leading the US input to 3GPP LTE standards making on behalf of the National Public Safety agencies.
NoC	Satellite Network Operations Centre
NPSTC	National Public Safety Telecommunications Council is a Federation of associations representing Public Safety telecommunications
NTIA	National Telecommunications and Information Administration (NTIA) is an agency of the United States Department of Commerce that serves as the President's principal adviser on telecommunications policies pertaining to the United States' economic and technological advancement and to regulation of the telecommunications industry
OPEX	Operational Expenditure
PMR	Private Mobile Radio technology provides group based radio communications for business and professional users
PPDR	Public Protection and Disaster Relief is a term that encompasses the traditional Public Safety organisations and also major incident rescue services
ProSe	Proximity Services - the 3GPP descriptor for Direct Mode (DMO) in LTE
PSS/PS	Public Safety Services or Public Safety - describes the emergency services and includes Police, Fire, Ambulance, Border Guards, Security Services etc.
RAN	Radio Access Network
RSPP	The Radio Spectrum Policy Programme (RSPP) defines the roadmap for how Europe can translate political priorities into strategic policy objectives for radio spectrum use
S-Band	Frequencies that range from 2 to 4 GHz
SDO	Standards Development Organisation
SIM	Subscriber Identity Module - is an integrated circuit that securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices
SLA	Service Level Agreement
TCCA	TETRA and Critical Communications Association (see www.tandcca.com)
TETRA	TErrestrial Trunked Radio - a digital trunked mobile radio technology
Tetrapol	A technology developed for the French Gendarmerie and in use by a number of Public Safety agencies in various parts of the world
UIC	Union Internationale des Chemins de fer' - the French-language acronym for the International Union of Railways
US	United States of America
UTC	Utilities Telecom Council – an Association of Utility organisations(in the USA)
VoLTE	Voice over LTE
VSAT	A very small aperture terminal (VSAT), is a two-way satellite ground station or a stabilized maritime VSAT antenna with a dish antenna that is smaller than 3 meters
Wi-Fi	A popular technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves

Version Control

Version No.	Date	Changes/additions made
1.0	December 2013	First published version