



# Mobile Broadband in a Mission Critical Environment – as seen from a TETRA perspective

## **Important Note**

The opinions and information given by the TETRA and Critical Communications Association in this white paper are provided in good faith. Whilst we make every attempt to ensure that the information contained in such documents is correct, the TETRA and Critical Communications Association is unable to guarantee the accuracy or completeness of any information contained herein. The TETRA and Critical Communications Association, its employees and agents will not be responsible for any loss, however arising, from the use of, or reliance on this information.

**First issued by the TETRA Association February 2011**

**Updated January 2012.**

## Introduction

TETRA is a well established technology and is in daily operation with thousands of mission critical and business critical organisations. It is clear that the unique “killer application” of TETRA is its ability to handle mission critical group calls. In addition, TETRA has a unique and unmatched list of special functions for professional users. When combined with superior voice handling it is not surprising that TETRA is the technology for mission critical users worldwide.

It has to be recognised that TETRA’s data capabilities are insufficient and, as a result, ETSI has created a wideband data standard which is known as TEDS (TETRA Enhanced Data Services). This standard will increase data throughput tenfold and products are now starting to appear that are TEDS capable. However, user organisations also need to be aware that more data throughput requires more spectrum. Even though spectrum regulation for TEDS is completed in CEPT countries, and users can today apply for spectrum from their national regulators, spectrum is not made available for TEDS deployment in a harmonized way. Although standard 25kHz channels can be utilised, wide bandwidth channels (50kHz and greater) are not generally available.

But spectrum is also the longest lead-time for availability of new technology, and for that reason, a number of user organisations have initiated work to have additional spectrum for even higher speed data services allocated for the Public Safety Services.

A number of organisations, such as ETSI, CEPT, the TETRA Association (now the TETRA and Critical Communications Association) and PSC-Europe have been working to gain recognition of the need for additional spectrum and this has resulted in a recommendation of future spectrum needs from the European Council of Ministers for Justice and Home Affairs.

All of this leads to a number of questions:

- When will more spectrum be made available?
- How much spectrum is required and can be reasonably justified?
- Where will the spectrum come from?
- Will the “Digital Dividend” be the answer?
- Could public networks deliver the data service?
- Which technology will it be?
- Public Safety organisations in North America have chosen LTE as technology – why not just use public LTE networks?
- Will higher speed data networks replace TETRA?
- If harmonized dedicated broadband spectrum is 5+ years away, what will we do in the meantime?

This paper – from the TETRA and Critical Communications Association dated January 2012 – will attempt to clarify how TETRA will fare when new high speed data technologies are being considered.

Currently there are two standards to consider – WIMAX and LTE. Over time LTE is expected to be the standard of choice for the public operators. As mentioned above, LTE is also the standard chosen in North America for broad band **data** services for the Public Safety Services.

LTE's main target is the nationwide mass market for public communication, so the first implementations will be focussed on large networks. It appears that WIMAX will become more of a niche technology and for smaller deployments.

With these new – so called 4G - technologies entering the marketplace, some proponents will naturally claim that their new technologies can replace all previous technologies and, in this case, that they are optimised to meet the needs of mission critical users. However, the reality may prove to be somewhat different.

Some of the options to consider are:

1. The ability to maintain an existing TETRA/TEDS wide area network in the allocated spectrum for mission critical voice and expand with a higher speed data overlay in areas where the need is most urgent.
2. Maintain TETRA wide area network in the allocated spectrum for mission critical voice and wait to expand with data from a wide area overlay network – when harmonized dedicated spectrum is available.
3. As 1 & 2, but using service from public operators for non-mission critical data needs to overcome the time and space constraints.
4. Replace an existing TETRA network fully with a LTE network – private or based on a public operator that has the capability to provide a “mission critical” grade of service.

This paper looks at the options available including the feasibility of delivering mission critical voice over an LTE network in a European context.

## Quick technology summary

LTE and WiMAX are 4G technologies which provide high speed data rates at much improved spectral efficiencies over older 3G technologies. Some of these improvements are due to the modulation and coding schemes adopted for these newer technologies, and some are also due to the use of smart antenna techniques.

There is no doubt that a technology such as LTE is a very effective way of passing data traffic at high speed in good signal conditions, and it is highly likely that LTE will be very successfully deployed in public networks for this purpose. LTE has also emerged as the chosen broadband data standard for Public Safety in North America.

Both LTE and WiMAX will satisfy growing demand for higher speed data services such as improved transmission of images and video, potentially moving into video conferencing and live broadcast reception.

Both technologies are scalable and can use different system bandwidths. However, typically expected deployments range from 1 x 5MHz, for example Time Division Duplex (TDD) WiMAX, to 2 x 10MHz for Frequency Division Duplex (FDD) LTE systems. In the wider bandwidth forms, up to 25Mbps is available for maximum downlink capacity, divided between the users of the cell. LTE also includes a 2x5 MHz dedicated (FCC 700 MHz band in US) option.

However, although WiMAX was designed as a TDD technology and LTE as a FDD technology both systems are now likely to be in both formats. Both standards will evolve and maybe eventually become one. Indeed a TDD version of LTE has already appeared. This will complicate spectrum planning.

In both cases, an adaptive modulation scheme is used, where the data throughput can be traded off against signal strength. This allows high data rates to be achieved when signal strengths are good, and increased ranges to be achieved at lower data rates. An effect of this is that the maximum quoted capacities can only be achieved closest to the cell site where the signal strengths are sufficiently strong to allow the highest rates of modulation. As the signal degrades towards the edge of the cell, the modulation rates are reduced, allowing communication to continue at lower signal levels, but with slower speeds. At the edge of a cell, one or two hundred kbps are available and this is also divided between the users of the cell if all of those users are at the edges of the cell.

Obviously, in order to deploy such technologies, a significant amount of spectrum is needed. Users can today actually deploy solutions in the GHz radio spectrum. However, that is not likely to be the best solution for nationwide deployment for Public Safety. For this application spectrum below 1 GHz would be needed as lower frequencies provide wider coverage.

Let us therefore consider some of the options:

## Option 1:

### **Maintain an existing TETRA/TEDS wide area network in the allocated spectrum for mission critical voice and expand with a higher speed data overlay in areas where the need is most urgent.**

As analogue TV is switched off around Europe and replaced with Digital TV, the so-called 'Digital Dividend' is freeing up TV frequencies around 800MHz which will be used to enable less expensive networks with fewer cells (compared to 2.5GHz and above), which could make more extensive geographic coverage economically feasible. However, none of these frequencies are likely to be allocated to mission critical users, and are likely to be auctioned off country by country to public network providers for commercial purposes.

Spectrum for broadband services can typically be found in the GHz area, but the cost of deployment at these frequencies will probably prohibit a wide area roll-out. As previously stated, the technology for smaller size networks that is available today is WiMAX. Combining TETRA / TEDS for wide area mission critical service with a dedicated WiMAX overlay is possible today – and actually implemented in some cases. LTE solutions for smaller networks are still some time out.

Given the currently available spectrum, an existing UHF technology such as TETRA still provides the only economical means to achieve wide area coverage, although clearly this cannot offer the same data speeds in unicast communications today as a 4G technology.

TETRA / TEDS is going to be the only viable **wide area mission critical data service** for many years – probably in excess of 5-10 years. A compromise where broadband coverage for exclusive mission critical use is needed would be to provide an overlay 4G network in metropolitan areas where there is sufficient density of mission critical users to justify the cost in network rollout.

TETRA will continue to be the standard for Mission Critical voice service for the next 10 years or more. There is no other technology on the horizon that is planned to deliver what TETRA does today.

Dedicated harmonized spectrum for broadband for Public Safety & Security organisations use are several years away – probably more than 5 to 10. That means that the only technology available for wide-area, mission critical data service for the next few years is TEDS<sup>1</sup>.

This option– with a hybrid solution – is a safe way forward.

---

<sup>1</sup> TEDS also requires spectrum.

## **Option 2:**

### **Maintain TETRA wide area network in the allocated spectrum for mission critical voice and wait to expand with data from an overlay network – when harmonized dedicated spectrum is available.**

This option is likely to stifle innovation and hinder organisational effectiveness for years, as this is the status quo. Indeed, this is described as one of the four development possibilities discussed in the Analysys Mason study into “Public Safety mobile broadband and spectrum needs”<sup>2</sup>.

Analysys Mason defined four possible evolution paths for the future demand of mobile broadband applications within the public safety sector as part of the study. Consideration of these different evolution paths demonstrated that the capabilities of current narrowband and wideband dedicated mobile networks used by the public safety sector will not be sufficient to meet future requirements under three of the four evolution paths that we defined. The only evolution path that could be accommodated by existing networks is the “steady growth” path. However, this is not sustainable in the longer term as there is growing evidence of trends and changes in working methods that suggest that it will not meet future demands.

The four evolution paths defined in the study indicate that a new generation of mobile broadband service is required to accommodate the range of future data, image and multimedia applications that public safety users will demand. The options for delivering this new generation of services include - making use of upgraded commercial networks (e.g. using HSPA+/LTE technology) with network deployment modified to meet the specific operational requirements of the public safety sector), or - developing a new generation of dedicated mobile broadband networks for exclusive public safety use.

This Option (2) will lead to “Minimal changes to existing operational practices, and limited scope to achieve greater efficiencies and responsiveness through new ways of working.”

## **Option 3:**

### **As 1 & 2, but using service from service providers for non-mission critical data needs to fill the time and space constraints.**

This option will make a data service available most of the time. The option, however, requires the user organisations to develop standard operating procedures (SOP) that takes into consideration that the data service might not be available when the user needs it most – i.e. when the public network is overloaded or not available. This is often the case during major incidents but could also happen with large events such as open air concerts.

---

<sup>2</sup> [http://www.tetra-association.com/Library/Documents/Files/Documents/Analysys Mason final report for TETRA Association 080310.pdf](http://www.tetra-association.com/Library/Documents/Files/Documents/Analysys%20Mason%20final%20report%20for%20TETRA%20Association%20080310.pdf)

## **Option 4a:**

### **Replace an existing TETRA network fully with a LTE network – either privately owned or based on a public operator that has the capability to provide “mission critical” grade of service.**

The use of LTE – the Long Term Evolution of GSM – could be postulated as a possible replacement for TETRA and other such standards to provide integrated voice and data facilities for public safety communication. A research study has shown that an LTE cell has the capacity to support multiple group calls. Unfortunately, when digging a little below the surface, many other factors will also need to be considered before a successful network can provide mission critical public safety voice communications in Europe in the future.

#### **Mission Critical Voice calls over LTE – can that be done?**

Replacing a TETRA network fully will require mission critical voice over LTE. Voice calls over an LTE network will be carried as voice over IP. Voice over IP has the advantage in that it is compatible with IP networks beyond the LTE network, and so can carry calls to and from fixed IP network users. However, using IP does add some penalty to the capacity of the network, as IP adds an overhead to the voice that it is carrying. The IP header overhead can be greatly reduced by compression, although compression sometimes does not work correctly in poor signal conditions as frames can be lost.

As there is no mature standard offering true multicasted mission critical group call performance (apart from TETRA), group calls are generally proposed to use a set of unicast IP streams, where each group member receives his own copy of the voice stream. This will cause group calls to load cells more heavily than individual calls in direct proportion to the number of users in the group on a call. The loading becomes worse where users are distributed near the edge of the cell, and will most likely cause an unexpected loss of capacity from the cell.

Whilst a fast call set-up over LTE may be theoretically possible, no demonstration of the performance in a loaded cell has been shown. Simultaneous unicast of group voice to a large number of users in one cell will create an excessive load.

The use of individual streams also means that the delay on received audio is slightly different for each user, which can lead to echo-like effects where users receiving the same call are standing near to each other.

The solution for this is to design a true multicasting function into the technology. Existing standards designed for mission critical use such as TETRA have voice embedded natively in the transmission format, and there is therefore no extra overhead. In particular they have true group calling, where the exact same transmission is received simultaneously by all members of the group, and therefore there is no extra capacity overhead whether one person or one hundred people receive the same call. If the LTE standards develop to provide this multicasting capability in the future, then it too will be able to support a more efficient means of providing a group call.

Companies with the expertise in mission critical systems are uniquely positioned to push this development. In the meantime, a solution to deploy high speed data (WiMAX or LTE) without the penalties caused by voice group calls is to deploy the 4G technology as an overlay network to carry unicast data services beside the core voice technology (TETRA).

A voice service – especially a group voice service – will be an overlay, and will be dependent on the application which contains this overlay. Mission critical group call has a lot more functionality than just the voice call itself. The following attributes are essential:

- Fast call set up – 300msec or less from PTT press on 95% occasions to call completion, which includes all subscriber actions and air interface transmissions (not just network response time).
- Priority levels for individuals and groups, which determine the order of access in high load conditions, and the order of pre-emption in emergency conditions.
- Emergency access – pre-empting other users if necessary.
- Queued calls in case not all sites have capacity for a call, and the ability to configure the conditions where the call will be queued.
- User prioritisation schemes which can determine the ability for a call to go ahead according to the presence of certain users
- Late entry – joining a call after it started
- Security requirements have led to a very specific and comprehensive functional suite including:
  - Static and Dynamic Keys
  - Group Cipher Key
  - OTAR and OTAK
  - E2EE
  - Terminal stun/kill (Remote disabling of lost or stolen terminals)
- and many other attributes

These features are not optional or “nice to have”, but features regarded as essential by Police officers in order to exchange information according to their confidentiality rules. Moreover, for a few Security Agencies it is even required to verify the correct implementation of such security features through checking of the product designs.

Most of these attributes can be added to an open standards process to ensure multiple vendor supply and sufficient competition in the market. There is no such development in the standards world yet. There is however at least one key attribute, which will have to be compromised – the 300msec call setup time – users would probably have to accept double or possibly triple this value, especially in emergency situations at heavy traffic load.

Further functionality is necessary on a mission critical network, such as:

- Direct mode – radio to radio communications outside the infrastructure
- Individual calls using half duplex PTT (push to talk) mode
- Status messages, which are used as fast efficient messages in addition to the more standard Short Data/Short Message text services
- Multiple levels of encryption, both end to end and air interface.
- Dynamic group management – providing groups over the air, temporarily or permanently
- Broadcast calls, both with static and dynamic user base
- Group scanning with talkback functions
- Paging from one service into another, and simultaneous services



- ....and so on....

Technology does not limit this – any application can be standardised. However standardisation can be a long process. The development of these standard applications for a real network will also take significant resources.

In the early years of a new technology, such as LTE, the focus will be on developments for the mainstream consumer and business markets rather than more specialist applications.

Direct Mode in particular needs special attention. A technology requiring several MHz of bandwidth per channel is not suitable for Direct Mode, especially where spectrum is constrained. The GSM-R community have overlaid a narrow band FM mode for such use. A similar alternative technology would be needed for an LTE handset.

An essential function for a mission critical network is the connection of dispatcher terminals via direct wired interfaces to the system. These devices fulfil specialised applications, inc:

- Monitoring multiple groups simultaneously
- Transmitting to single or multiple groups simultaneously
- Transmitting broadcast calls to single or multiple groups
- Having a raised priority in calls, to be able to override the current transmitting users if needed
- Patching groups together
- Encryption with:
  - Static and Dynamic Keys
  - Group Cipher Key
  - OTAR and OTAK
  - E2EE
- Terminal stun/kill
- System management functions
- Open interfaces to third party command and control applications.

These devices and their interfaces to the network will also have to be developed before a full solution can be suitable for mission critical use.

There is no reason why LTE or WiMAX standards cannot be expanded to incorporate these extra levels of functionality but currently there is no activity in that area.

## Option 4b:

### **Replace an existing TETRA network fully with a LTE network – based on a public operator service.**

One of the issues in deploying a high speed data network is the cost of deploying a privately owned and maintained system that offers service over a wide area in the available spectrum, as described in the previous section. To avoid the capital costs of deploying such a network, or where there is effectively no spectrum available for private network deployment, service could be obtained on a public carrier network – with the consequences to operation service clearly understood.

The issue of public vs. private networks has been explored in some detail over recent years, as alternatives to dedicated technologies such as TETRA have been considered. Public networks are often not an attractive solution, and most studies raise the following issues related to coverage:

- A public network provider will want to invest in coverage where the population resides and, therefore, where the revenue generation is. In consequence there is little incentive to invest in areas of low population density. The cost of network expansion may have to be borne by the public safety community alone.
- The public safety community will – through a tender process – have to select one of the providers, and fund the expansion of that system to provide the required degree of coverage. That in turn will distort competition and could be the basis for litigation. One way around that would be to have access to all networks and roam between them, but that opens up other problems, including having to broadcast data on multiple networks in parallel.
- Bespoke mission critical networks are usually designed with higher degrees of resilience, including multiple levels of fallback with emergency power supplies, alternate link routing and local call switching even within a single base station. These facilities are not provided to the same degree on a public network.
- In conditions of local or national emergency, public networks typically become overloaded as their normal customer base naturally wants to communicate at the same time. It can be difficult to guarantee access for the public safety community in these conditions.
- In high threat conditions, e.g. terrorist threats or in times of war, public networks can be deliberately switched off to prevent terrorist communications for coordination or for remote activation of attacks.
- Network security and protection against cyber attacks in dedicated government information networks is required at a much higher level than in public networks.
- Operators may have difficulty with having to withhold disruptive network maintenance for example due to an incident i.e. an operator would need to consult with public safety organisations before being able to disrupt services and this could have a major impact on its overall competitiveness.

To overcome these issues a public network would have to be built in an unusual way (for a commercial operators) to provide the levels of resilience and fallback communications that would be required for all conditions. It is questionable whether a commercial operator would be willing to commit to such a network design?

Governments, who have bought mission critical nationwide service based on TETRA have typically specified non-functional requirements such as very high degree of availability, extensive coverage, control over service supplier, financial constraints, stiff penalties etc. Specifications that a main-stream operator simply would not and could not accept.

### Terminal devices

Proponents of public network technology will often cite the tremendous volumes of terminals sold and claim that this will enable a much cheaper terminal to be made and sold for niche markets, such as public safety users.

However this position has proven to be untrue in previous examples. The same claims were made for handsets for the GSM-R technology (GSM for railways). In practice, the requirements for such terminals were sufficiently different from standard terminals, and the volumes sold so small that they have actually worked out very much more expensive – and considerably more expensive than terminals designed for the TETRA market. This is because the niche GSM-R market has far fewer terminals and many fewer competing suppliers than that of the TETRA market.

Terminals for mission critical use differ from a mass market cellular terminal in many ways:

- They must be rugged, and be resistant to shocks and vibration. Most professional terminals will be dropped onto a hard surface many times in their lifetime – they must remain fully operational through such events and must survive without damage.
- They must be designed for a wide variety of environmental conditions. Typical public safety terminals are designed to meet IP54 or higher levels of moisture and dust protection (and must maintain this level of protection when shocked or dropped as above). Typical temperature ranges run from -10C to +60C – with full functionality.
- They must have excellent audio output – typically 1W of audio for operation in high ambient noise conditions
- They must be able to sustain a high duty cycle receive condition with periodic transmit for the duration of a 10 hour shift – this dictates a large battery, which must be easy to remove and charge.
- They must support a wide range of accessories including vehicle kits, remote speakers and microphones, and the accessories need to be equally as rugged as the terminals themselves.
- Niche market terminals are needed, for example Intrinsically Safe terminals to operate in explosive atmospheres, and covert terminals for surveillance use. The terminal market must be diverse enough to support these, otherwise the technology itself will fail.
- They must support Direct Mode operation outside the network, and also operate with separate repeaters and gateways to communicate from Direct Mode back into the network.

These requirements dictate that the terminal design differs quite widely from a normal cellular market terminal.

The radio chipset may be common with a normal cellular handset but overall terminal cost will be significantly higher than consumer devices as re-use of the LTE platform has minimal impact on the overall costs.

## Spectrum, coverage and network cost

Public operators planning LTE deployments typically need up to 20MHz of spectrum<sup>3</sup>. Frequencies can be reused in different sectors on a site, but to achieve best coverage, different spectrum is required in each sector. If mission critical users wish to own or manage a network for their exclusive use, they will need to obtain this spectrum. Unfortunately, there are no current assignments identified for exclusive public safety use at frequencies below about 2.5GHz in Europe which can accommodate this bandwidth. TETRA systems are deployed in 400MHz. Propagation range at 400MHz can be more than ten times greater than the equivalent range at 2.5GHz, which mean that a network at 2.5GHz or above will need tens (or potentially even hundreds) of cells for every 400MHz cell. A mission critical network typically needs in excess of 95% geographic coverage of a region or country. The cost of deploying this may be unsupportable for a private network funded entirely by public safety due the cost of the number of cells needed. This need for a large number of cells also requires a large number of links (which each need high bandwidth to support broadband data) and a suitably large switching platform.

---

<sup>3</sup> Response by GSA - Global mobile Suppliers Association to Ofcom Consultation: Award of available spectrum: 2500-2690 MHz, 2010-2025 MHz and 2290-2300 MHz (Date of GSA response: March 9, 2007)

Pag.5 Question 8....By taking into account technology innovation over the next 10 years, we recommend a cap that should allow up to 2 x 20 MHz per single FDD operator or 30 - 35 MHz per single TDD operator. Such block sizes will facilitate the introduction of LTE (Long Term Evolution) high broadband datarate services, as they are under discussion in 3GPP and by the wireless industry.....

## Summary

TETRA will continue to be the standard for Mission Critical voice services for the next 10 years or more. There is no other technology on the horizon that is planned to deliver the functionality that TETRA does today.

Dedicated harmonized spectrum for broadband that could be used by Public Safety & Security organisations is several years away – probably more than 5 or even 10. This means that the only technology available for wide-area, mission critical data service is TEDS<sup>4</sup>.

However, LTE or WiMAX may provide a very effective overlay network which provides high speed data coverage in areas where there is sufficient density of mission critical users to justify the cost of a privately operated network. These overlays are likely to be deployed in metropolitan rather than in rural areas and in 2.5GHz or 3.5GHz spectrum.

Public networks may also offer solutions for mission critical users, and these avoid both the cost of the capital outlay in deploying a network and the issues in obtaining spectrum. For public networks to be useful, the issues of network resilience and fall back communications must be addressed, together with those of communications security in the design of those networks. Conscious decisions must be made concerning guaranteed availability in periods of high network load and during disaster conditions.

The operator will need to have the skills to provide “mission critical” grade of service. If this cannot be achieved then applications will need to be restricted to those that are non mission critical. In addition, Standard Operating Procedures (SOPs) will need to be developed and also users will need to be trained in how to act when the service is un-available.

In the long term, no matter which technology provides broadband data, and whether that technology also integrates voice services, it can only be successful if terminal devices match the requirements of the mission critical market. Ruggedness, environmental protection, audio levels, battery life, accessories and so on are all vital factors in addressing this market. These factors make it difficult to reuse terminals taken from the consumer market and to obtain the economies of scale that the consumer market brings.

---

<sup>4</sup> TEDS also requires spectrum.