Report for the TETRA Association

Public safety mobile broadband and spectrum needs

Final report

8 March 2010

16395-94

analysys mason

Contents

Analysys Mason Limited
Bush House, North West Wing
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)20 7395 9000
Fax: +44 (0)20 7395 9001
enquiries@analysysmason.com
www.analysysmason.com
Registered in England No. 5177472

1 Executive summary

This is the final report of a study conducted by Analysys Mason Limited ('Analysys Mason') for the TETRA Association, to undertake a review of future mobile broadband needs for public safety mobile communications, and how these needs might be addressed.

For the purposes of this report, the term 'public safety' is assumed to comprise primarily police, fire and ambulance services, although the requirements are also considered to be applicable in a wider Public Protection and Disaster Relief (PPDR) context.

The majority of public safety users in Europe currently use dedicated radio networks for their mobile communications that have been designed specifically to meet their needs, typically using digital mobile communications technologies such as TETRA or TETRAPOL and operating in spectrum in the 380–400 MHz band. These networks offer a range of low rate data services, but the speed and capacity that is available within those networks limits more widespread use of higher-speed data applications.

In line with societal trends for access to information on the move, public safety operations are becoming increasingly information-driven, requiring access to a wider range of wideband and broadband applications. These range from high-quality imaging to uploading and downloading of large data files, and real-time video.

Given the limitations in capacity of existing dedicated networks to deliver mobile broadband services, it is considered likely that a new generation of solution will be required across Europe in the next five to ten years, to meet future public safety user demands. This new solution, if delivered using new dedicated mobile broadband networks that are designed to meet public safety requirements, will require additional spectrum to deliver the services required.

In order to define the benefits of the development of a new generation of dedicated mobile broadband networks for public safety, and to support the identification of additional spectrum to meet future needs, the TETRA Association has commissioned Analysys Mason to undertake this study to gather information on future public safety user requirements, based on a review of existing documents and reports that have been published in Europe over the past few years and are available in the public domain.

We have reviewed each of the documents (listed in Annex B), with a view to determining:

- the future mobile data and multimedia applications that are envisaged to be in widespread use within the public safety sector over the short and medium term
- the network requirements that are associated with these applications, i.e. the operational requirements of mobile communications networks that will meet public safety user requirements

- the benefits to the public safety sector of the development of a next-generation of dedicated mobile data networks (requiring additional, dedicated spectrum to deliver), compared to the alternative options such as re-engineering of existing or planned commercial networks in Europe.

The authors of this report would like to thank the TETRA Association for their inputs to this study and identification of the relevant documents and reports that have formed the basis of the study's recommendations.

1.1 Summary of applications and user requirements

Current and future public safety mobile data and multimedia applications identified in the various reviewed documents cover a range of needs, including:

- mobile office
- transfer of images
- biometric data
- automatic number plate recognition
- digital mapping and location services
- remote database access
- personnel monitoring
- sensor devices/networks
- remotely controlled devices
- non-real-time video
- real-time video.

Summary of operational requirements essential to public safety mobile communications

The reviewed documents make reference to a number of specific operational requirements that are essential for public safety mobile communications, in order to ensure the availability, reliability and integrity of networks. These include:

- high levels of network availability
- high degree of network control, including the ability to implement prioritised access for specific user groups or individuals, and to reserve capacity where required
- near nationwide geographic coverage, including the ability to communicate in remote areas
- security
- low latency, specifically end-to-end voice delay of no more than 200 milliseconds
- interoperability between different public safety authorities and across borders
- highly resilient networks, including various layers of redundancy
- ability to support mixed traffic.

1.2 Summary of evolution of applications in the public safety sector

There are number of key trends apparent within the daily routines of public safety users, as well as in improved responsiveness at major planned and unplanned events, which are affecting the public safety sector's future mobile data requirements:

- ways of working are changing
- data is being used to enhance voice
- command and control is moving from command centres to the field
- there is greater awareness and use of multimedia.

These trends have been used to develop four alternative evolution paths to illustrate how future use of mobile data and multimedia applications might develop within the public safety sector, as summarised below in Figure 1.1.

Evolution path	*Description*
Steady growth	Working methods change slowly, and voice remains the dominant method of mission critical communication. Existing data applications continue to be used alongside this, with a gradual increase in use.
Data enhances voice	Incident response increasingly relies on situational awareness provided through a range of data applications on the move, and access to a range of faster data applications that can be used in a similar net-centric fashion to that of group-based voice calls (i.e. group sharing and exchange of data).
Information driven	A common operating picture is established at incident scenes through use of mobile command centres alongside central command units, and sharing of information (including voice, text, images, data and video) between the two. This drives requirements for real-time uploading and downloading of information (images, data) between field and control rooms, including use of video conferencing and other on-demand video services to aid communications and incident response.
Full multimedia reliance	A diverse range of mobile broadband applications, including high-quality imaging and real-time video applications take off, with widespread use across the public safety sector. Widespread information sharing improves the establishment of common operating pictures at incidents, facilitates real-time decisions at incidents, and enables the introduction of new video services such as remote medical applications, and personal characteristics recognition.

Figure 1.1: Evolution paths to illustrate alternative views of how future usage might evolve [Source: Analysys Mason]

Our assessment of the implications arising from each of the evolution paths in terms of future network requirements is summarised in Figure 1.2 below.

Evolutionary path	*Outcome*	*Implications*
Steady growth	Minimal changes to existing operational practices, and limited scope to achieve greater efficiencies and responsiveness through new ways of working.	Public safety users will require longer-term retention of existing dedicated networks to meet voice, narrowband and wideband data functionally, however these will be insufficient to meet future mobile broadband needs. This will constrain the development of new working methods and use of a wider range of data and multimedia applications. Limited additional sector-wide benefits are gained through migration to better, faster and more responsive ways of working, but overall growth in data usage is limited by network constraints.
Data enhances voice	Public safety users benefit from significantly greater situational awareness at incident scenes, through sharing and exchange of a range of data and images. Security of data transfer becomes increasingly significant, which limits the usefulness of commercial networks to carry sensitive data traffic.	Existing dedicated narrowband and wideband networks will be insufficient to accommodate the volumes of data traffic that will occur in everyday use. Commercial networks are not deployed to meet the operational requirements for mission-critical data applications, such as secure data transfer, nationwide coverage, guaranteed availability and control. This supports the need for a new generation of dedicated mobile broadband network designed to meet the operational needs of mission critical data.
Information driven	Mobile officers and those in command centres have access to a common picture of incident operations, facilitated by sharing of data, images and other information. This improves decision making, responsiveness and the ability of public safety officers to work in crisis situations, as well as to respond to everyday incidents. Applications such as fingerprint recognition, licence plate recognition, and access to criminal records can all be conducted remotely, in real time.	The need for data applications to be delivered over networks that ensure high availability, resilience and secure communication, and are as reliable as existing TETRA/TETRAPOL voice networks, is increased as a result of the need to access a wider range of applications from anywhere, at any time. Networks must be capable of mobile broadband information upload and download. The need for a more extensive range of mobile applications therefore requires capacity enhancement, similar to the “data enhances voice” path, which will be beyond the capability of existing dedicated networks.
Full multimedia reliance	New ways of working are implemented across the public safety community. A new generation of situational awareness applications are used in daily response as well as for major incidents. Public safety users are able to operate more efficiently, making better use of resources and reducing unnecessary travel. Real-time video is widely used – for example, video calls between mobile command and central command units, real time CCTV image transfer, and remote medicine applications.	With the evolution in data and multimedia applications, and the requirement for those applications to be available over a very wide area (to make applications such as remote telemedicine feasible), existing narrowband and wideband networks will have insufficient capacity and functionality to meet the requirements of this evolutionary path. Similarly, there are limitations in use of commercial networks due to a lack of full geographic coverage, capacity and ability to carry secure data. This evolutionary path therefore requires the development of a new generation of dedicated mobile broadband networks to deliver more network capacity, higher bitrates and a wider range of applications.

Figure 1.2: Impact of different paths on future network requirements [Source: Analysys Mason]

1.3 Summary of options to meet public safety's evolving requirements

It appears that the capabilities of existing narrowband and wideband dedicated mobile networks currently used by the public safety sector will not be sufficient to meet future requirements under three of these four evolution paths. 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 since there is already growing evidence of changes in working methods and trends within the public safety sector that suggest that this path will not match future demands.

A summary of the four alternative evolution paths and their impact on network requirements is provided in Figure 1.3 below.

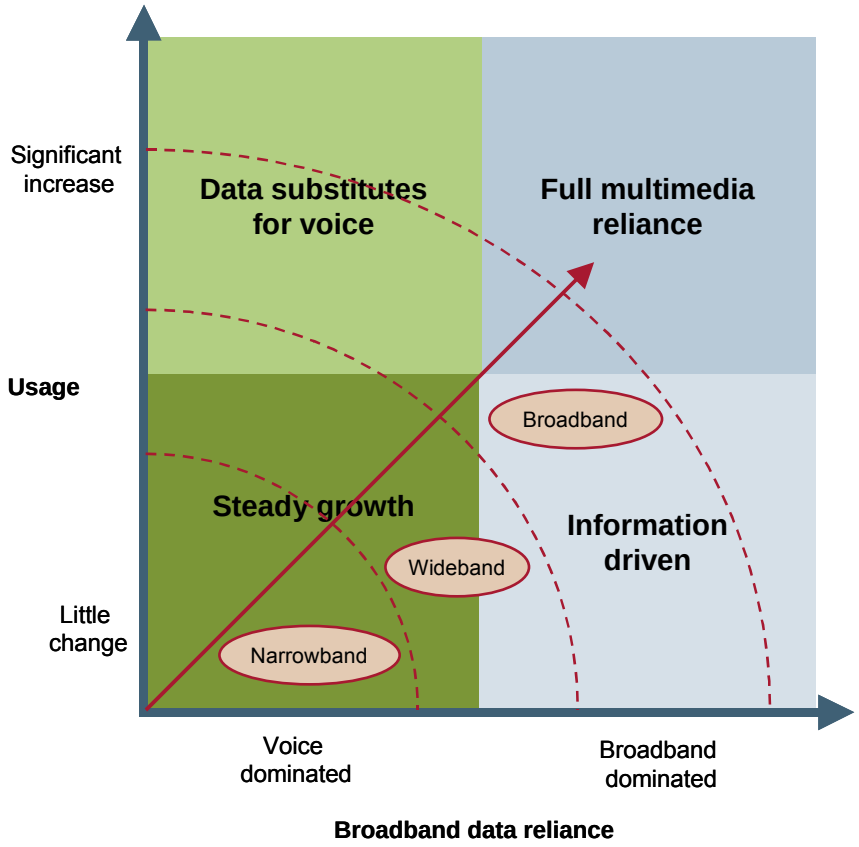

Figure 1.3: The four alternative evolution paths and their impact on network requirements [Source: Analysys Mason]

The four evolutionary paths 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 are to make 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 to develop a new generation of dedicated mobile broadband networks for exclusive public safety use.

While the new generation of data service could theoretically be delivered through upgrading and re-engineering commercial networks, the reviewed documents suggest that this might not be achievable in practice, based on a number of reasons, which range from technical limitations through to cost and commercial considerations.

In particular, there are a number of reasons why commercial operators might be unwilling to make the necessary network changes to support public safety operational needs:

- the public safety sector requires very extensive geographic coverage as well as in-depth coverage penetration inside buildings, irrespective of location, which does not match the typical roll-out requirements of a commercial network
- it is likely to be very expensive to re-engineer commercial networks to achieve all of the public safety sector's operational requirements, and there are questions about whether sufficient incentives exist for commercial operators to do this. For example, typically requirements include the need for battery back-up to be available at thousands of base station sites across the network, and for networks to be designed to ensure that they are highly resilient (including overlapping coverage, standby power supplies and fallback sites) and that no single 'point of failure' exists either in access or core networks
- there are questions about whether some of the public safety requirements are actually achievable
- there is a question about whether the required Grade of Service for public safety use can be guaranteed within a network shared with commercial users, particularly in times of very high traffic loading
- there are conflicting views on whether signalling could be encrypted over the air interface in 3G/LTE
- ensuring the specific requirements for carriage of 'restricted' or 'confidential' documents requires careful network planning and approvals, which is complex and costly to achieve
- it is not clear that networks can be dimensioned to achieve the required immediacy and guaranteed access that public safety requires.

In addition, the reviewed documents presented a further range of reasons why public safety users have been reluctant to make more widespread use of existing commercial networks, and have favoured the development of their own dedicated networks. These include the following.

Coverage	Commercial operators typically invest in coverage where populations exist, and capacity is designed to maximise revenue generation in those areas, with little incentive to invest in areas of low-density population. Public safety, by contrast, requires ubiquitous coverage across a country's geography for everyday use, irrespective of population densities.
Network design	Re-engineering of commercial networks to meet public safety's requirements might be feasible in theory, but in practice would result in large parts of the commercial network being heavily over-engineered. This is likely to be more costly for the public sector to fund than a dedicated network provisioned to meet the specific coverage and capacity needs of the public safety user based, without having to provision for additional commercial traffic.
Sabotage	There is a view that commercial networks might be more vulnerable to sabotage by criminals that dedicated networks are, if the network is known to be used for public safety communications. Dedicated public safety networks are typically more guarded against sabotage through a range of specific measures (e.g. vetted staff, secure fencing at sites, and networks designed to ensure no single point of failure in the event of sabotage, etc.).
Rollout schedules	There are precise requirements for the roll-out of public safety networks (e.g. the need to align with police/fire/ambulance area boundaries), which do not match typical commercial roll-out strategies.
Risks of shared use	There are risks such as information security, quality of service and control of service level agreements if public safety users share networks with commercial users, which previous experience suggests can be avoided through use of dedicated networks under government control and supervision.
Reliance on commercial operators	There is a reluctance for public bodies to be reliant on a fully commercial operator, in view of the potential lack of control upon future network investment, business plans and financing[1].

1.4 Conclusions

The study has found that, in line with societal trends evident within today's Information Society, a diverse range of data, imaging and multimedia applications are in demand within the public safety sector. Demand for access to a wider range of information is being driven by changes in working practices, which is creating requirements for access to a far wider range of data sources (textual, images and video) that is typical in commercial mobile networks. Sharing of various data types (textual, images, video, etc.) is being used in order to establish and maintain a common operational picture between agencies and between field and central command staff. This is being used to improve responsiveness, aid the deployment of resources, and improve timeliness and decision making in daily public safety operations and when responding to major planned or unplanned events.

Three of the four evolutionary paths developed for this study illustrate the public safety sector's need for a next generation of mobile broadband network to deliver the range of applications that are envisaged in the future. As there is a limit to the range and volume of data and multimedia applications that existing dedicated narrowband and wideband networks, and existing commercial

[1] This is referenced, for example, in ETSI TR 102 628 (SRD on additional spectrum requirements for future PSS wireless communication systems in the UHF frequency range, which refers to specific conditions in place in a number of European countries

networks, can provide, if a new generation of mobile broadband network is not made available, some new applications cannot be delivered. Ultimately, this will affect how already emerging changes to ways of working within the public safety might evolve, and, in the longer term, constrain the further development of the sector.

A new generation of services could in theory be delivered using an upgraded commercial network, with the deployment of the network engineered to meet specific public safety requirements. However, as explained in Section 6.2, this option does not appear to be achievable in practice. The only other option is to encourage industry to develop a new generation of mobile broadband networks for dedicated public safety use. To enable the industry to devote the necessary investment to develop new dedicated networks, there is a need for additional spectrum to be identified, since existing bands are already fully utilised by existing dedicated public safety systems. It should be noted that identifying suitable spectrum is on the "critical path" to support development of a new generation of dedicated mission critical mobile broadband solution, because of the timescales associated with identifying suitable spectrum.

This additional spectrum demand is based upon the combination of the various factors identified throughout this report, specifically:

- trends in the range of data and multimedia applications in demand within the public safety sector
- potential increase in user densities and intensity of use for data applications
- specific traffic characteristics of public safety operations (e.g. network-centric ways of working)
- the infrastructure and technical requirements to meet the operational requirements of the public safety community (e.g. availability, security, reliability, latency), and limitations in use of commercial networks to deliver these.

Given the cost of deploying new networks, access to spectrum in bands below 1GHz will ensure maximum commonality with existing dedicated networks deployed in the 380–385/390–395MHz bands, facilitate re-use of assets where possible (e.g. radio sites). Use of spectrum above 1GHz (e.g. bands around 2 GHz) might be feasible but would incur significantly higher roll-out costs compared to that below 1GHz, raising questions at national government level as to whether and how the additional costs can be funded.

Based on the reviewed documents, the European dimension to the public safety spectrum requirement is important for a number of reasons:

- the public safety sector is a niche market and therefore benefits from the identification of harmonised spectrum even more than commercial mobile systems (e.g. GSM or UMTS), because of the smaller user base and resulting lower volumes of equipment and terminals

- even if commercial solutions are adapted to meet specific requirements of a niche sector such as public safety, there are still costs involved in the necessary modifications, and therefore harmonised spectrum availability is key to ensure that manufacturers are able to develop

products for a European market. An example of the re-engineering of existing commercial standards to meet niche requirements is that of GSM-R (the railways version of GSM) – although the GSM standard is supported by all major vendors around the world, GSM-R equipment is supplied by relatively few and the availability of harmonised spectrum for the product has therefore been important to reduce costs

- interoperability is an increasingly important requirement within the public safety sector, both to communicate between different public safety authorities within a country, and to communicate across borders. This is evidenced by a number of the documents reviewed for this study.

The lack of available spectrum is therefore a significant barrier to the further development of mobile communications capabilities tailored to meet public safety requirements, until such time as a new, harmonised band can be identified at a European level.

2 Introduction

This report has been prepared by Analysys Mason Limited ('Analysys Mason') on behalf of the TETRA Association, to present the results of a study to review the future needs and requirements for mobile data and multimedia applications within the public safety sector.

For the purposes of this report, the term 'public safety' is assumed to comprise primarily police, fire and ambulance services, although the requirements are also considered to be applicable in a wider Public Protection and Disaster Relief (PPDR) context.

The public safety sector uses a variety of communications networks at present, including a range of fixed voice and data systems within headquarters (HQ), and digital mobile networks while on the move. The majority of public safety users in Europe use dedicated radio networks for their mobile communications that have been designed specifically to meet their needs, typically using TETRA or TETRAPOL digital mobile communications technologies and operating in spectrum in the 380–400 MHz band.[2] This is the frequency band identified at a European level for digital public safety communications as a result of ERC/DEC/(96)01 and subsequent decisions.

While the public safety sector has traditionally relied on voice communication as its primary means of communication at incidents, making particular use of group calls, as well as Direct Mode Operation (DMO) and air to ground voice communications, the requirements for access to a range of mobile data applications have evolved over recent years and are now considered to be an essential part of the public safety sector's mobile communications. This is evidenced, for example, by the dependency on applications such as automatic number plate recognition (ANPR) and access to various databases by police while on the move.

The public safety sector currently has two options to address the use of a wider range of data applications:

- to upgrade existing narrowband networks to provide a wideband overlay (e.g. TEDS), providing wideband data capability
- to continue to make use of existing dedicated networks for mission critical voice and low speed data, and use commercial networks to deliver higher bandwidth, non-mission-critical[3] data.

---

2 In many countries in Europe, public safety users also make use of existing commercial networks (e.g. GPRS or 3G) in addition to dedicated TETRA/TETRAPOL networks. Commercial networks are often used for the provision of additional vehicle and handheld data services, typically of a non-mission critical nature. This is because commercial networks are not designed to meet the specific functional requirements for mission-critical public safety communications, which requires very high levels of network availability, low latency, very wide area coverage and various levels of security and encryption.

3 "Mission-critical" refers to a service or information for which failure to deliver, disruption or delay is not tolerable in view of its impact on public safety operations.

However, neither of these options is envisaged to meet public safety requirements in the future, since there is a need for a mobile broadband solution that can deliver mission critical high speed data, requiring a network that is designed to meet the specific operational requirements of the public safety sector. Underpinning support for the development of a next-generation of mission critical mobile broadband solution is the identification of suitable spectrum to deploy future systems. This is required because the existing spectrum available for public safety mobile communications is already fully deployed to accommodate today's narrowband and wideband networks.

The TETRA Association has therefore commissioned this study to provide an assessment of future public safety user needs, which will determine future spectrum requirements. Since much of the required information on future public safety needs exists in a range of documents and reports that have been published in Europe over the past few years, the scope of this study has not been to conduct new research into potential future user requirements, but rather to summarise the requirements that are already known to exist through a review of the existing documents.

The remainder of this document is laid out as follows:

- Section 3 describes our overall approach to the study.
- Section 4 reviews the current and future requirements and needs of the public safety sector
- Section 5 considers alternative trends of how public safety needs might evolve
- Section 6 presents the results of our analysis, in terms of options to meet future public safety requirements
- Section 7 presents our conclusions from the study.

The report includes a number of annexes containing supplementary material:

- Annex A provides a list of the acronyms used in this document
- Annex B provides the list of documents that have been reviewed as part of this study
- Annex C includes a summary of our review of each document.

3 Approach to the study

The overall approach to the study is summarised in Figure 3.1 and a brief description of each task is provided below.

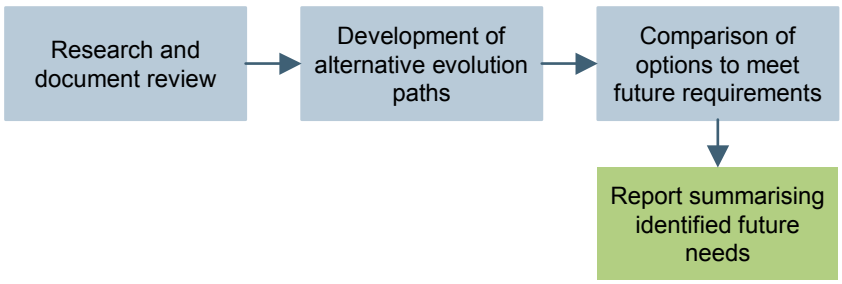

Figure 3.1: Approach to study [Source: Analysys Mason]

Research and document review

In this task, a wide selection of documents from a range of public-domain sources (listed in Annex B) were reviewed and used to provide an overall assessment of public safety user needs, and the associated benefits from use of dedicated mobile broadband networks to meet those needs. A summary of the findings from this document review is provided in Annex C.

An objective of this task was to review the forecast demand for data and multimedia applications as presented in the range of existing documents recommended by the TETRA Association for inclusion in this study, including assumptions on requirements for dedicated networks and the benefits of using dedicated networks compared to a shared network.

Development of alternative evolution paths

The first aim of this task was to identify which applications are considered to be driving demand for a new generation of mobile broadband networks for public safety use. This was achieved by summarising the range of applications that were presented in the reviewed documents and grouping them into similar application types.

The second aim of this task was to develop a series of alternative trends for the development of public safety user needs, illustrating how usage might evolve under different alternative views of the future. Four alternative evolution paths were developed, ranging from a steady-growth base case (i.e. continued and slightly increased use of existing applications) to a much greater reliance on a range of traffic types (voice, data and media) within mission-critical environments.

Comparison of options to meet future requirements

In this task, the options available to the public safety sector for providing mobile broadband services were summarised. In addition, the limitations of existing dedicated networks and existing commercial networks to deliver the range of requirements illustrated by the alternative evolution paths were identified, and the public safety user requirements that a new generation of mobile broadband network need to meet were considered.

Report summarising identified future needs

The results of the analysis are contained in the remainder of this report, which forms the main deliverable from the study.

4 Summary of applications and user requirements

4.1 Current and envisaged future mobile applications

Based on an assessment of the currently used applications within the public safety sector, along with those envisaged to be used in the future, it is apparent that public safety mobile communications have traditionally been voice-based, but there is a trend towards using a range of data applications alongside traditional voice applications to enhance communications.

Traditional voice services are widely used for mission-critical mobile communications, and often used in a 'network-centric' fashion[4], evidenced by the widespread use of group calls. Various documents[5] indicate that the requirement for these services will likely continue to exist. The range of voice services that public safety users rely on includes:

- group calls
- encrypted individual and group calls, with authentication
- individual calls to command centre PABX and/or public telephone networks
- direct mode operation between terminals (i.e. terminal-to-terminal communication, without a network)
- emergency calls
- air-to-ground communications.

It is now apparent that a range of data, image and video applications are emerging alongside these traditional voice services, and there is an increasing demand for these data-based applications to be used alongside voice for mission-critical communications, in many cases in a similar 'network-centric' manner to voice.[6]

Examples of emerging applications are described in Figure 4.1 below.

4 "Network-centric" refers to sharing of information between people and devices in a many-to-many (group) configuration, as is often used within the public safety sector.

5 For example, as referred to in results of TETRA Association TEDS workshop, 2007.

6 For example, personalised data is being shared amongst different users at an incident scene, which can offer benefits such as improving the situational awareness of officers at a scene. There is also a trend towards mobile offices, and mobile command and control.

Application	*Description*
Mobile office	Access to mail and intranets, transmission of incident reports from an incident scene or remote location, etc.
Transfer of images	A very wide range of image requirements, including high quality images of damage within buildings, detailed buildings plans, photographs of potential criminals, personal recognition systems (e.g. facial, iris), images of lost children, injuries at incident scenes and other incident-related images required for subsequent evidential purposes.
Biometric data	A greater range of personal recognition systems including fingerprint, facial and iris recognition of potential criminals by officers on patrolling duty, and transfer of this information in real time to HQ/command centres to be checked against biometric records. This improves the efficiency of the potential identification of criminals.
Automatic number plate recognition	A camera captures licence plate details and transmits the image back to HQ/ control centre. This is an application that has emerged in widespread use in a number of countries over the past few years, and its use is expected to continue. Transferring the image back to HQ/command centre enables officers to verify whether the vehicle is stolen, or involved in a crime or other offences. In future, this application could be extended so that image capture and checking against information contained within police databases could be conducted entirely by officers while on patrolling duties, in real time.
Digital mapping and location services	Tracking of vehicles or people, precise geographic positioning (e.g. similar to applications that are provided on commercial mobile handsets to enable navigation and identification of nearest location of interest).
Remote database access	Remote database checks of various types, used increasingly within the public safety sector to retrieve information from databases stored in HQ/command centres by offices on patrol or at incidents. Other databases that could be accessed in real time to support incident response include the Fire Service 'Gazetteer'.
Personnel monitoring	Monitoring of public safety officers in real-time to monitor health conditions while responding to incidents (e.g. fire fighters within a building, or officers involves in search and rescue operations). Other applications might include perimeter monitoring (e.g. of people entering/leaving an incident scene), vehicle or personal alarms, or tracking the location of an assigned individual for general personnel management purposes as well as in the event of an emergency.
Sensor devices/networks	Sensor networks deployed in specific incident areas, used to collect data or images within the area for onward transmission back to HQ/command centres (e.g. collection of thermal imaging from inside buildings reporting on the state of fire or other damage). Fixed or mobile sensors used to record data and images in real time (including images in a video-streaming format), which could then be distributed to other officers at the same incident (e.g. via a sensor network at the incident scene), or back to HQ/command centres. This enables officers in the command centre to have access to the same images as the officers at the incident, enabling real-time decision-making.
Remotely controlled devices	Robotics devices, used to record images within badly damaged buildings that are too unstable for officers to enter, or to operate within explosive areas or in underwater searches. Other applications include remotely turning on or off surveillance microphones or surveillance cameras (including remotely aiming or pointing the camera), and activating and de-activating alarms. Various telemetry systems also in use or envisaged within a range of public safety usage scenarios include control of moving fixed assets (e.g. vehicles, equipment in hospitals, etc.).

Non-real-time video	Capture of video streams at the scene of an incident, which are then stored (e.g. in a vehicle) and downloaded when the vehicle returns to HQ. Could also refer to slow-scan video used to gauge activity at an incident scene, but which is not of sufficient quality to be used as evidence or to support real-time decision-making.
Real-time video	Real-time video surveillance from fixed cameras permanently located along streets and in buildings or from portable cameras mounted on vehicles. Other applications include transmission of video from field officers to command centres, and vice versa, and uses within the health sector, such as remote medical services (e.g. treating patients in rural areas using video calls between the patient's home and the health centre) or treatment of casualties at an incident using real-time transfer of images between responders at the incident area and doctors in hospitals who are able to provide guidance on remote treatment at the incident scene or while the patient is in an ambulance being transported to hospital.

Figure 4.1: Summary of the range of current and future public safety mobile data and multimedia applications [Source: Analysys Mason]

The increase in data, image and video applications is driving, and will continue to drive, demand for greater bandwidth and increased functionality from public safety mobile networks.

A summary of the range of applications that are in current use within the public safety sector, along with their approximate intensity of use (on a scale of high to low use), is provided in the ERO summary of responses to its questionnaire on public safety and disaster relief produced for CEPT FM PT38, as reproduced in Figure 4.2 below.

Intensity of use	*Application*
High	Geo-location identification (of vehicles and people)
	Database query/access
	Short data/messaging
	Direct mode communication
	Image/video/map/plan/photo transfer
Medium	Group calls
	PSTN calls
	Air-to-ground communications
	Command and control (dispatch)
	Data from ambulance to hospital
	Emergency call
Low	WAP queries
	Email and mobile office
	Calls to/from PSTN and office PABX
	Tracking (e.g. RFID)
	Priority call/access
	Trunked operations
	Fire applications
	Video calls
	Radio paging

Figure 4.2: Summary of applications in CEPT WG FM38 survey response [Source: ERO]

A similar range of applications is identified in other documents, such as the ETSI Technical Specification (TS) on requirements for communications between authorities/organizations during emergencies (ETSI TS 102 181). This document also includes a different range of applications, which have been defined in terms of their impact on network throughput, timeliness (i.e. latency) and robustness. This is reproduced in Figure 4.3 below.

Service	*Throughput*	*Timeliness*	*Robustness*
Email	Medium	Low	Low
Imaging	High	Low	Variable
Digital mapping/GIS	High	Variable	Variable
Location services	Low	High	High
Video (real time)	High	High	Low
Video (slow scan)	Medium	Low	Low
Remote database access	Variable	Variable	High
Database replication	High	Low	High
Personnel monitoring	Low	High	High

Figure 4.3: Data services table from ETSI TS 102 181 [Source: ETSI]

Usage scenarios

Various documents[7] include a number of detailed usage scenarios within the public safety sector, which illustrate the range of applications that might be used within daily operations, or to respond to specific incident types. A summary of usage scenarios contained within the reviewed documents is provided in Figure 4.4 below.

7 Operational scenarios are described in a range of documents including references 9 (Mesa), 11 (WIK), 13 (Euler) and 17 (Safecom) – see Annex B.

Figure 4.4: Examples of usage scenarios within public safety [Source: Analysys Mason]

Usage scenario (source)	*Summary of applications used*
Patient services for a car crash (US Department of Homeland Security)	• Video conference call set up between the ambulance and the hospital • Ambulance's geo-location, along with vital measurements and treatments of the patient, recorded from the ambulance and transmitted wirelessly to the hospital
Major explosion/bomb (MESA/TS 70.001 v3.3.1)	• GIS used by police to establish the perimeters for the incident scene • Initial casualties information forwarded to hospitals, including images of injuries taken at the incident scene • Real-time video feeds relayed to the control room of the incident area • Fire fighters enter damaged buildings using bio-telemetry devices to monitor people and conditions within the building • Robotic devices used to confirm that no other explosives are present • Crime scene diagrams constructed using portable laptops at scene of incident • Images recorded as evidence by investigators at the scene
Traffic stop (US Department of Homeland Security)	• Situation message, police vehicle's ID and geo-location transmitted from police car at the scene of incident to other offices and to command centre • Suspect's licence plate read and sent to command centre, and queried against several databases located at HQ • Results from database query send back to police car • Video stream of the action at the incident transmitted and stored in central database, and made available on demand to dispatch/command centre. Onward message sent to other offices, along with video footage, to arrest the suspect • Arresting officer's ID loaded onto RFID handcuffs • Suspect's biometric data taken at incident scene, stored and forwarded to command centre • Case report sent electronically from arresting officer's car
Large earthquake in urban area, with many damaged buildings (MESA)	• Virtual treatment centre set up at incident scene; buildings surveyed for damage and identification of locations of further casualties • Handheld computers used to sketch building structures, entrances, etc. • Mobile command centre set up • Hazardous zones identified in buildings; fire fighters equipped with personal monitors and location tracking devices to enter hazardous areas

Large international finance summit (scenario developed by a UK agency)	• Mobile command centre established at venue, for in-building communications and to establish perimeter control, linking to central command units of police, fire and ambulance authorities • Establishment of a common operating picture using a range of data types (images, text, voice, video) • A range of mobile broadband at-venue applications available including o Enhanced personal recognition systems (iris, facial) o Ability for ambulance service to send high-quality video streams from the venue and from vehicles to hospitals, if required o Ability for fire service to send high-quality video streams from venue to command centre (e.g. in-building plans, structural plans, etc.) o CCTV camera images captured from the venue and distributed to central command centres in real time o Ability to track people and objects within the venue
Large fire in a high rise building (TR 102 485 : Technical characteristics for Broadband Disaster Relief applications (BB-DR) for emergency services in disaster situations)	• A scenario involving fire and rescue and police rapid response – within a concentrated area of 1km^2 • Personnel protection and surveillance using sensors with panic alarms • Thermal image video capture and transmission • Asset tracking within the incident area • Video surveillance across the incident area • Perimeter zone control to track all cars going in and out of a fixed location • Data capture and control devices to capture or deliver data to the point of decision within the incident area • Back office applications enabling a range of business functions within the area

All of the above examples suggest that future public safety operations will rely on the availability of multiple data, imaging and video applications as well as voice, and demonstrate the necessity for applications to be supported within a single network, to ensure interoperability between different public safety authorities/organisations involved in the response of a specific incident.

4.2 Operational requirements essential to public safety mobile communications

Public safety networks have features that are distinct from those of commercial networks, as they need to be able to support mission-critical applications that have unique technical and operational requirements such as extensive coverage, capacity, reliability, immediacy of communications, security, redundancy and resilience. Other requirements also include the ability to support non-voice applications (in real time and non real time), interoperability within the organisation, as well as other emergency services, and cross-border communications.

The documents and reports that were reviewed make reference to a number of these operational requirements, as summarised in Figure 4.5 below.

Requirement	*Summary*
Availability	Availability in time is specified as three or four 'nines of availability' (e.g. 99.98% or better at all times) for some users. Others specify different requirements for different times, such as 99.9% per year, 99.7% per month and 99% per 24 hours (e.g. as referenced in CEPT FM38 questionnaire response on PPDR from the Denmark administration). This high degree of availability includes access to networks in all areas at all times (including under very high traffic loading conditions during which it may be necessary to reserve capacity for specific incident responders).
Control	A high degree of network control is required (e.g. to enable prioritised access or reserved capacity to be guaranteed when required) [8]. Control requirements also include the ability to queue traffic, and to manage queuing conditions and update these in real time.
Coverage	Public safety network coverage requirements differ from those of commercial networks, which are typically designed to cover areas where populations live (and therefore may provide near-100% population coverage, but do not provide the same level of geographic coverage). The public safety sector, by contrast, requires much wider geographic coverage, and the availability of the same set of applications across all geographies. Coverage must also be consistent with typical organisational boundaries within the various public safety services. Coverage requirements are specified as, for example, 99.5% (outdoor mobile), 65% or better (indoor mobile), 99.9% (air to ground).[7]Another document from a UK agency refers to at least 99% of the landmass of Great Britain needing to be covered (including offshore islands).[7]
Security	Security requirements are guided by national security and accreditation requirements, which vary in different countries. TETRA provides different layers of encryption including over-the-air and end-to-end (better than 80-bit encryption is referred to in documents we have reviewed). Other security features include two-way authentication.
Low latency	There are requirements for very short call set-up times and for limited end-to-end voice / data transmission delay (for mission-critical applications). One document refers to end-to-end voice delay being no more than 200 milliseconds.[9]

8 E.g. referenced in various replies to the ERO questionnaire on PPDR on behalf of CEPT WGFM PT38 and in ETSI TR 102 628

9 For example, as referred to in various replies to ERO questionnaire on PPDR of CEPT WGFM PT38.

Interoperability	There is an established need for different units within the public safety sector to interoperate (e.g. police, fire and ambulance, and associated services), requiring each to use the same technology. In addition, there is a growing awareness of the benefits of cross-border interoperability between different public safety units operating in different European countries.
Resilience	Networks must be highly resilient and include various layers of redundancy. Central network switching must be fully redundant, with geographically distributed switching. Interconnection between base stations must also be fully resilient and include back-up lines between key base stations. Back-up power supplies are required at different levels – for some key sites, there is requirement for up to seven-day back-up in some instances. Key base stations sites (i.e. a selected number of sites from within the overall network) need to have fallback sites available in the event of failure of the primary site.
Ability to support mixed traffic (i.e. voice and data)	An integrated network solution providing support for transmission of mixed traffic types (e.g. voice, data, images) is a requirement for public safety, in order to be able to use the same technology in all environments (e.g. ranging from day-to-day emergency response to major planned incidents and major disasters/unplanned incidents).

Figure 4.5: Public safety mobile communications operational requirements [Source: Analysys Mason]

These essential operational requirements are unlikely to change in the future, and moving forward a more diverse range network-centric requirements might be envisaged, based on increasing use of sensors and sharing of information, images and video. In particular, the occurrence of various major incidents around the world has reinforced the need for core operational requirements to be maintained in current and future-generation of public safety networks.

While future commercial networks (e.g. LTE) may be able to offer the required range of data services that are envisaged to support the usage scenarios described in Section 4.1, there will still be challenges to ensure that the operational requirements of the public safety sector can be met, particularly as commercial networks are typically optimised for financial return on investment rather than to deliver services across a wide geography (irrespective of population centres), which is what the public safety sector requires.

At present, commercial networks are not deployed to meet the core operational requirements for public safety use for a number of other reasons:

- commercial coverage, even for GPRS, is typically not nationwide and is often limited inside buildings
- 3G and LTE are likely to be deployed in ‘islands’ of coverage, rather than nationwide
- roll-out of sites will not be at a pace or geographically suited for a public safety network
- queued calls and the ability to control/configure queuing conditions is not provided
- there are no provisions in current standards for pre-emption capabilities or preferential measures which would guarantee capacity for public safety users in times of heavy traffic
- there are no provisions for two-way authentication or integral Direct Mode (i.e. terminal-to-terminal capability)
- there are potential issues with transporting secure information over a shared public network, both in relation to over-the-air conveyance and end-to-end encryption

- redundant switching is required for public safety applications, which commercial networks do not always guarantee
- no single point of failure must exist within the network
- high availability is not guaranteed (e.g. three or four nines of availability at all times is a typical requirement for public safety applications).[10]

[10] Availability in time is also specified as 99.9% per year, 99.7% per month and 99% per 24 hours in the Danish response to the ERO questionnaire on PPDR.

5 Evolution of applications in the public safety sector

5.1 Trends in the use of mobile applications in the public safety sector

The public safety sector is following the same trends that are apparent within the wider society for access to a wide range of information on the move, and sharing of knowledge and information.

This, and a number of other trends evident within the public safety sector, is driving demand for mobile data requirements, as summarised in Figure 5.1 below.

Changes to ways of working	Ways of working are changing within the public safety sector – for example, there is a trend towards mobile command and control to enhance the effectiveness and efficiency of incident response. This is driving demand for simultaneous access to a much wider range of applications, which are being used in combination to respond to an individual incident.
Data enhancing voice	Public safety users are increasingly using data applications to enhance the mission-critical voice communications that they rely on for daily use and when managing planned and unplanned major events.
Information-driven operations	Usage scenarios for how public safety users work on a day-to-day basis while out on patrol or away from command centres suggest that usage is evolving towards greater sharing of information from a variety of sources (voice, data and video). The overall purpose and objective of this way of working is to establish common operating picture between all public safety agencies and between officers at incidents and those in HQ command centres, thus improving situational awareness. This has many benefits including better mobilisation of field teams, more timely response and more accurate information available to support decisions on incident response.
Greater awareness and use of multimedia	Increasingly more daily routines are taking advantage of a mixture of different traffic types (i.e. voice, data, images, video), which is supported by the trends towards mobile field operations and mobile offices. This requires access to the same range of applications while in the field as an officer would have while in a command centre. Multimedia applications extend across different network types, from wide-area transmission across field boundaries, through to local area transfer of incident-specific information, to personal area networking and the collection and transfer of data collected by remote sensors and/or tracking devices.

Figure 5.1: Trends affecting public safety sector requirements [Source: Analysys Mason]

The reviewed documents indicate that the range of applications in demand within the public safety sector is extending significantly beyond the 'traditional' core, group-call-based voice and data applications that have been previously associated with the sector. Interactive multimedia services, access to office applications while on the move, and a range of sensing, robotic and telemetry applications are all in demand. In addition, over time it is expected that both the range and the

intensity of use of different applications will increase. This requires much higher data speeds and additional dedicated network capacity to be available, with applications being accessible through handheld devices used indoors or outdoors, and to vehicle-based users.

5.2 Alternative evolutionary paths

To explore how demand for different applications might evolve over time, and the impact of this evolution on network requirements (i.e. availability, speed and capacity), a series of alternative evolutionary paths for the public safety market have been developed. These have been built based upon the consensus regarding the range of applications that might be used within the public safety sector in the future, as ascertained from the reviewed documents. This is illustrated in Figure 5.2 below, with the applications shown in comparison to their impact on network capacity requirements (i.e. low to high capacity requirement) and their estimated stage of development (i.e. available now or envisaged in next 3–5 years).

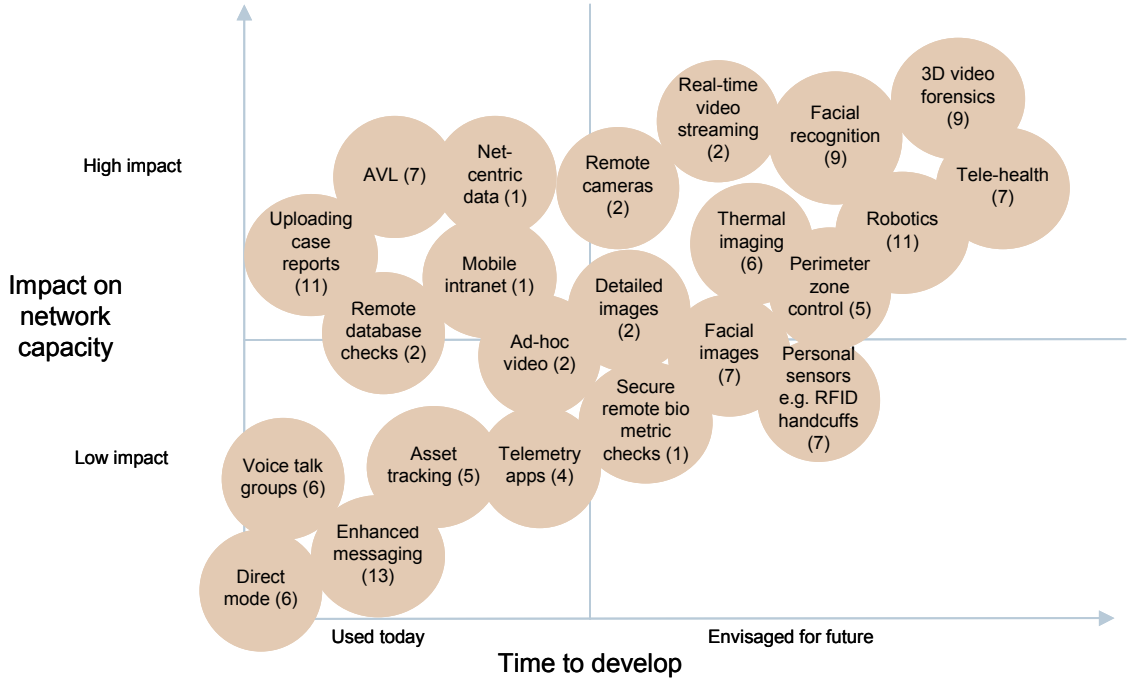

Figure 5.2: Illustration of how demand for multimedia applications might evolve within the public safety sector, and impact on network capacity [Source: Analysys Mason, various documents[11]]

Specifically, based on the envisaged range of applications in demand within the public safety sector, and an estimation of the time necessary for them to develop into full operational use, we

[11] Numbers in brackets refer to documents listed in Annex B which make reference to the various applications illustrated in this diagram.

have developed four alternative views of how data and multimedia applications usage might evolve.

These four evolutionary paths are summarised in Figure 5.3 and described in more detail below.

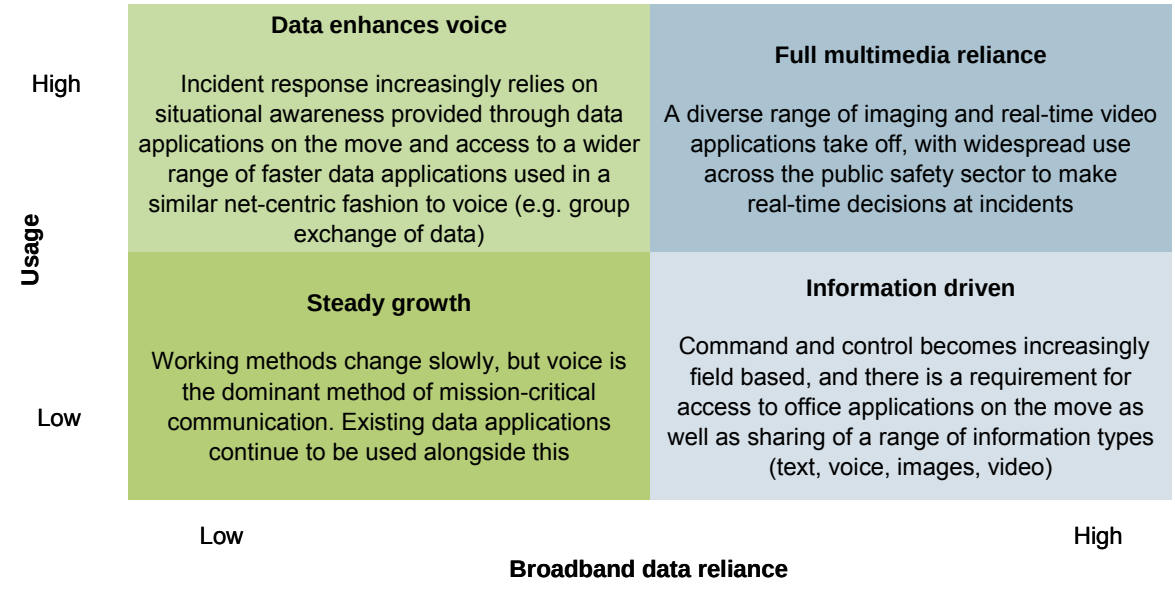

Figure 5.3: Four alternative evolution paths for use of data and multimedia applications within the public safety sector [Source: Analysys Mason]

5.2.1 Steady growth

The "steady growth" path represents the base case for market evolution within the public safety sector, under the assumption that there are no major changes to requirements or significant deviations from currently observed usage trends.

In this evolutionary path, there is a continuation of current usage patterns already evident within the sector, with a wider range of data applications being used alongside group-based voice calls. This combination of traffic types (i.e. voice and data) is evident both in daily operations and in responses to major incidents, however, mission-critical communications continue to use voice as the main delivery method, using established networks. Data usage continues to grow, but at a slow pace, constrained by lack of availability of dedicated, secure, data capacity that meets the public safety sector's core operational requirements. The communications strategy is therefore to continue to use the existing generation of dedicated TETRA network, upgraded to TEDS where practical, alongside commercial networks that are used to carry non-mission-critical data. However, it is unlikely that this strategy can be sustained indefinitely, given that the intensity of data usage will inevitably increase in line with current trends (evidenced, for example, by the significant increase in use of ANPR in recent years).

A summary of the implications of this evolutionary path is provided below.

Trend	Continuation of existing trends with greater volumes of data use, but constrained by lack of suitable networks to deliver mission-critical data in high volumes.
Outcome	Minimal changes to existing operational practices, and limited scope to achieve greater efficiencies and responsiveness through new ways of working.
Implications	Public safety users will require longer-term retention of TETRA and TEDS networks to meet voice, narrowband and wideband data functionally. This will constrain the development of new working methods and use of a wider range of data and multimedia applications. Limited additional sector-wide benefits are gained through migration to better, faster and more responsive ways of working, but overall growth in data usage is limited by network constraints.

Figure 5.4: Summary of "steady growth" evolutionary path [Source: Analysys Mason]

5.2.2 Data enhances voice

A key driver of the market for public safety applications is the trend towards network-centricity in data and multimedia operations. Similar to when using group-based voice calls, public safety users have a requirement to share data and multimedia applications on a many-to-many basis in order to ensure that everyone involved in a specific incident response is fully briefed on all information and decision making is undertaken accordingly. This manifests in the increasing demand for use of data to improve situational awareness, gained from a mixture of telemetry, sensor and video applications.

The "data enhances voice" path represents this trend of demand for access to data in combination with voice, used in a network-centric way. This path can therefore be summarised as being an extension of the current trends for greater access to data applications being used alongside voice, but with data applications becoming increasingly essential to mission-critical responsiveness. Over time, it is expected that a gradual reduction in group-based voice calls will occur as more and more communication takes place via transfer of data and images.

A summary of the implications of this evolutionary path is provided below.

Trend	Data is used alongside voice to enhance flow of information occurring in daily public safety activities and for incident response. Widespread adoption of data applications means that the capacity available on existing dedicated TETRA/TEDS networks is not sufficient to carry the data traffic that will be generated.
Outcome	Public safety users benefit from significantly greater situational awareness at incident scenes, through sharing and exchange of a range of data and images. Security of data transfer becomes increasingly significant, which limits the usefulness of commercial networks to carry sensitive data traffic.
Implications	Existing dedicated narrowband and wideband networks are not sufficient to accommodate the volumes of data traffic that will occur in everyday use. Commercial networks are not able to deliver the required functionality to accommodate secure data transfer, or the capacity or coverage to achieve the necessary network-centric ways of working. This supports the need for a new generation of dedicated mobile broadband networks.

Figure 5.5: Summary of "data enhances voice" evolutionary path [Source: Analysys Mason]

5.2.3 Information driven

There is consensus amongst various reviewed documents that there is trend towards mobile command and control – in other words, enhancing traditional HQ-based command centres with mobile command centres that are set up to respond to specific events on a daily basis, or set up to assist the smooth operation of major planned events (e.g. New Years Eve celebrations, major sporting events, etc.). This drives demand to establish a common operating picture between the venue/incident and central control rooms, achieved through sharing of various information (voice, images, video). In addition, knowledge-based working requires public safety officers to have access to the full range of applications available to them in the office, whilst in vehicles or on the move.

These applications could be accessed using hand-held devices or through vehicle-based devices. Users will require immediate access to information stored in databases in order to manage command and control from the incident scene. The direction of data is both uplink (in order to transmit various images, data and video from the scene of incidents to central command) and downlink (e.g. from command centre to the incident scene, to assign resources or respond to information requests). There will also be a greater demand for mobile office applications to complete incident reports remotely rather than upon returning to HQ/command centres. As with the "data enhances voice" evolution path, there will be a greater demand for access to a wider range of data and imaging applications to enhance situational awareness and responsiveness. This will include sensory devices to gather information on conditions of buildings and people, and the ability to exchange this information wirelessly between different incident responders. Greater volumes of mission-critical data traffic will therefore emerge, which cannot be delivered by commercial networks operating on a 'best efforts' basis.[12]

[12] 'Best efforts' in this context refers to data that can tolerate delay or interruption, i.e. is non-mission-critical.

As with the "data enhances voice" evolution path, the "information driven" path will generate data volumes that will exceed the capabilities of existing dedicated narrowband and wideband networks, and require a new generation of dedicated mobile broadband networks.

A summary of the implications of this evolutionary path is provided below.

Trend	There is a demand for access to the same range of applications in the field as those available at HQ/command and control. This includes widespread use of mobile office applications, as well as remote access to databases and ability to view, replicate and update information in real time.
Outcome	Mobile officers and those in command centres have access to a common range of situational pictures, data and other information. This improves responsiveness and the ability for public safety officers to work in crisis situations, as well as to respond to everyday incidents. Applications such as fingerprint recognition, licence plate recognition, and access to criminal records can all be conducted remotely, in real time.
Implications	The need for data applications to be delivered over networks that ensure high availability, resilience and secure communication, and are as reliable as existing TETRA voice networks, is increased as a result of the demand to access a wider range of applications from anywhere, at any time. The need for a more extensive range of mobile applications therefore requires capacity enhancement, similar to the "data enhances voice" path, which is beyond the capability of existing TETRA and TEDS networks.

Figure 5.6: Summary of "information driven" evolutionary path [Source: Analysys Mason]

5.2.4 Full multimedia reliance

In the "full multimedia reliance" path, there is a dramatic increase in both the range and intensity of use of new and innovative data and multimedia applications, including video streaming which is necessary for real-time interactive services such as telemedicine, 3D video forensics and high-quality evidential facial recognition applications. Public safety users start to make significant use of video applications alongside voice and data, driving demand for a wide range of applications to be made available over a common network interface to aid interoperability. Similar to the "data enhances voice" scenario, there is a widespread take-up of a range of data applications used in a network-centric manner. Alongside this, however, video streaming is used to further improve situational awareness at incidents and to enable a common operating picture to be established (e.g. through use of video conference calls, live CCTV video footage streaming, etc.). Future applications such as telemedicine are rolled out to improve access to medical services in rural areas. This requires access to a mobile broadband network covering a wide geographic area in order to reach the remotest areas, since the public safety organisations cannot control where unplanned incidents occur. New ways of working fully evolve so that there is substantially less reliance on HQ/command centres to store, retrieve and deliver information, since users are able to access a full range of applications while on the move.

As with the "data enhances voice" and the "information driven" paths, this evolutionary path will generate data volumes that will exceed the capabilities of existing dedicated narrowband and wideband networks, and require a new generation of dedicated mobile broadband networks.

A summary of the implications of this evolutionary path is provided below.

Trend	There is full reliance upon a wide range of traffic types (voice, data, video) in order to respond to new ways of working, and roll-out of new services such as remote telemedicine and 3D forensics. There is widespread take-up of a wide range of mobile data applications similar to the other evolution paths, alongside new multimedia applications.
Outcome	New ways of working are implemented across the public safety community and users are no longer constrained by having to return to HQ/command centres to complete certain tasks. A new generation of situational awareness applications are used in daily response as well as for major incidents. Public safety users are able to operate more efficiently, making better use of resources and reducing unnecessary travel.
Implications	With the evolution in data and multimedia applications, and the requirement for those applications to be available over a very wide area (to make applications such as remote telemedicine feasible), existing narrowband and wideband networks have insufficient capacity and functionality to meet the requirements of this evolutionary path. Similarly, there are limitations in use of commercial networks due to a lack of full geographic coverage, capacity and ability to carry secure data. This evolutionary path therefore requires the development of a new generation of dedicated mobile broadband networks to deliver more network capacity, higher bitrates and a wider range of applications.

Figure 5.7: Summary of full multimedia reliance evolutionary path [Source: Analysys Mason]

5.3 Mapping of applications to the four alternative evolutionary paths

The range of applications detailed in the various documents reviewed for this study have been mapped to the four alternative evolution paths as described above, in order to provide examples of how the use and range of applications might develop across the different evolution paths.

This mapping is summarised in Figure 5.8 below. Note that the numbers in brackets indicate references to the documents listed in Annex B. It should also be noted that since voice requirements are assumed to remain constant across all of the four evolutionary paths, voice is not included in the mapping table, although it is assumed to remain as an essential requirement for public safety operations.

Figure 5.8: Mapping of data applications to trends [Source: Analysys Mason]

Application	*Steady growth*	*Data enhances voice*	*Information driven*	*Full multimedia reliance*
Mobile office	Status messages, either field to field or command to field, are delivered by email in addition to short data/short messages, for resource allocation and incident control [2, 3, 6]	Emails/office applications are used for administrative messages, and access to emails and intranet whilst out of the office improves timely response to requests [1, 2, 17]	Increasing access to web applications (e.g. Intranet and Internet, online access to contacts databases etc.) is made, enabling incident reporting to be handled via mobile devices, reducing the need to return to HQ/command centre to access office applications [2, 5, 6, 17]	Incident-specific information exchanged using web applications (e.g. language translation, web-addressable cameras) in addition to use of a wide range of Mobile Office applications (contacts databases, email, Intranet) [5,17, 18]
Database queries/updates	Database checks conducted in vehicles and via hand-held devices (e.g. passport information, Gazetteer, criminal records, patient records) [1, 2, 6]	Increased ability to updated databases with textual inputs in real time to provide additional incident details, or patient record updates whilst on the move [1, 2, 17]	Additional data updates provided from incidents and uploaded in real time (e.g. visual information, results of biometric checks) [6, 17]	Increasing upload/download of data and updating in real time (e.g. ECG traces) plus development/update of architectural plans of buildings from incident scenes [7, 8, 11]
Location-based applications	Use of geographical positioning tools (e.g. GIS) [2, 6, 8]	Asset tracking (e.g. of people and equipment) with positional information sent periodically to HQ/command centre [2, 6, 7]	Increasing use of self-forming networks (e.g. perimeter tracking at incident scenes and machine-to-machine communications) [1] [2] [6]	Fully integrated tracking / surveillance / image systems used in real time (e.g. to record location and status of fire fighters and people within a building), along with video robotics (e.g. to capture information in explosive environments) [6]
Digital mapping	Used for navigation and access to digital maps [2]	Access to 3D geographic images [1, 2]	Increasing use of images of different types and quality e.g. aerial views of incidents, high quality imagery [1, 2,5]	Live 3D views inside buildings, and mapping of personnel and casualty locations [9]

Biometric monitoring	Use of basic telemetry applications [2, 5]	RFID used for tracking of personnel at incidents [2, 5, 7]	Biometric monitoring of personnel conditions over time [5, 7, 11]	Body worn sensors (e.g. object impact on helmet or vest, RFID-handcuffs) providing real time monitoring and information updates, improving real time structural awareness [7, 17]
Still images	Image and audio capture at incidents (e.g. push images of suspects and missing persons to field officers and images of fingerprints stored in central databases) [1, 2, 6]	Gathering of evidence at crime and incident scenes, and collation of witness information using field devices (e.g. incident scene photo transfers) [1, 2, 7]	Transmission of building floor plans and use of thermal image capture and transmission [1, 2, 7]	Evidential-quality image capture, and/or very detailed images (e.g. burns or other injuries [1, 7, 11]
Slow scan video	Sequence of fixed images exchanged between command centre and officers in the field [2, 6, 11]	Limited motion video captured and available on demand to command rooms and dispatch [5, 6, 7]	Video conference calls between field and command centre to support incident response and decision making [6, 9, 11]	Information captured by surveillance cameras at incident scenes relayed to command centres in real time, forming an essential element of mission critical communications and decision making [17, 18]
Real-time video	Relaying of ad-hoc video and surveillance camera information to control cars responding to incidents, and real-time traffic flow monitoring [7, 11, 19]	Upload of real-time standard definition video (e.g. from cars or handheld devices to command centre) [5, 7, 11, 19]	Live high definition, mission critical video footage transferred between incident and command (e.g. from ambulance to hospital), and use of mobile video conferencing [2, 6, 8]	3D video forensic applications, telemedicine and sophisticated airborne video platforms communicating with mobile devices [6, 8, 17]

6 Options to meet public safety's evolving requirements

6.1 Options to provide mobile broadband services to the public safety sector

As demonstrated in the previous sections, the various documents reviewed for this study indicate a general consensus that a wide range of data and multimedia applications will be required to meet future user demands within the public safety sector. The four alternative evolutionary paths developed for this study illustrate how demand for those applications might evolve over time, in line with changes to ways of working that are already evident with the public safety sector, such as a greater demand for mobile working, and increasing sharing of information to establish a common operating picture, often requiring upload of significant volumes of data of different types (e.g. images, video).

The options available to the public safety sector to deliver the envisaged range of applications under the different evolution paths are as follows:

- continue to use the existing generation of dedicated networks, and upgrade those to deliver wide band functionality (e.g. using TEDS).
- continue to use existing narrowband and wideband networks, and use existing commercial networks to provide additional, non-mission critical, data services
- develop a new generation of mission-critical mobile broadband network solution, either by developing a new generation of dedicated mobile broadband network or by upgrading existing commercial networks (e.g. based on HSPA+/LTE) and engineering their deployment to deliver the required public safety operational requirements of availability, coverage, security and control.

From our analysis, it is clear that, with the exception of the "steady growth" path, each of the other evolution paths will require additional high-bitrate data and multimedia applications beyond the capabilities of existing dedicated narrowband and wideband networks. Similarly, current commercial networks will not be able to support the range of envisaged applications, and in any case will not, as current deployed, meet the operational requirements of the public safety sector in terms of wide area coverage, security, resilience, control and availability.

There is growing evidence of the need for public safety to access multiple data applications simultaneously in order to establish a common operating picture, which requires use of a common infrastructure to avoid the need for multiple handsets and solutions. This is particularly true in the case of responding to major incidents, which require much more intensive use of a wider range of applications but using the same equipment and networks that are used in daily public safety operations. The combination of existing dedicated networks and existing commercial networks does not meet these requirements.

The advancement of network functionality requirements in line with the alternative evolution paths developed for this study is summarised below.

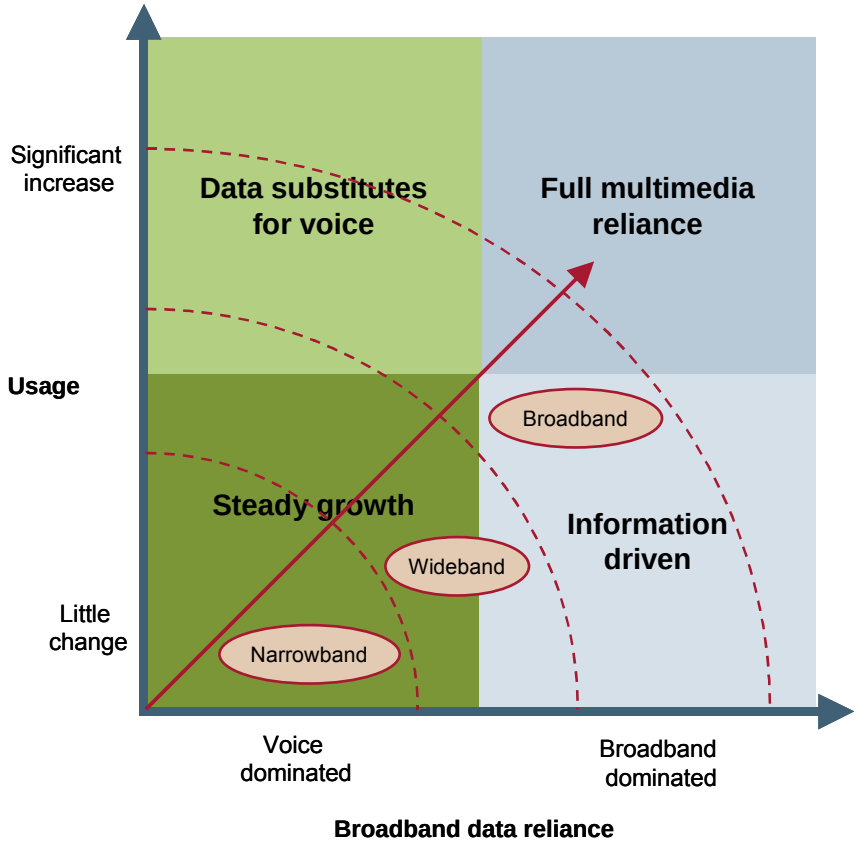

Figure 6.1: The four alternative evolution paths and their impact on network requirements [Source: Analysys Mason]

As described in Section 5.2, it appears that the "steady growth" path cannot be sustained indefinitely, given that the intensity of data usage is already increasing in line with current trends (evidenced, for example, by the significant increase in use of ANPR in recent years). This suggests that the only feasible option to meet the future evolution of public safety user requirements is to develop a new generation of mobile broadband network.

This conclusion is further evidenced by the range of usage scenarios that various documents envisaged within the public safety sector, as described in Section 4.1. The range of applications in concurrent use within these different usage scenarios demonstrates that, without a new generation of mobile broadband service being available, the full range of applications within the various scenarios will not be available in practice. This is summarised in Figure 6.2 below.

Figure 6.2: Benefits of the development of a new generation of mobile broadband services for public safety use [Source: Analysys Mason]

Usage scenario	*Existing public safety networks*	*Existing public safety networks plus commercial networks*	*Upgraded commercial network or new dedicated mobile broadband networks*
Patient service at car crash	Limited bandwidth to deliver video calls and images of patient injuries from ambulance to hospital, resulting in less timely response	Transferring sensitive patient records between ambulance and hospital not possible over commercial networks due to security and bandwidth limitations, leading to less timely response, and more manual paperwork	Faster identification of crash location, transfer of patient details in real time means improved emergency service response and enables more rapid diagnosis and treatment
Major explosion	Many of the envisaged applications not supported by current networks due to lack of bandwidth and limited data rate (e.g. incident perimeter tracking, real-time video feeds and bio-telemetry), resulting in less timely response, need for more resources and manual recording of information	'Best effort' nature of commercial networks means that they cannot be relied on in major incident situations. Public safety users are limited to using applications available on their dedicated networks, resulting in reduced interoperability, need for more resources, additional manual paperwork and reduced ability for crisis management	Interdepartmental communications maintained through secure, interoperable network, and network dimensioning to enable network-centric voice and data transfer improves efficiency of operational response to major incidents and more effective resource deployment, awareness and management
Traffic stop	Limited ability to capture and transmit information from the scene. ANPR in use today but increasing volumes of use mean that there are capacity constraints	Secure transfer of personal information not possible over a public network, reducing ability to capture and transfer information from the scene and possibly reducing ability to apprehend the criminal	Real-time identification of suspects and criminals, more timely response and better crime response rate
Earthquake	Mobile command and virtual treatment centre not possible using current generation of networks, leading to less effective, slower response, duplication of information and reduced ability to make real-time decisions	Levels of commercial traffic in this urban area would be high and so it is unlikely sufficient capacity can be dimensioned for public safety use. Loss of benefits such as slower response and duplication of information	Virtual treatment centre made possible through availability of higher speed, dedicated capacity leading to real-time diagnosis and treatment, better use of resources, and reduction in ambulance-hospital journeys
Fire at depot	This operational scenario illustrates that the only reliable mission critical communication methods at present are voice and low-speed data, limiting responsiveness and flow of information	'Best effort' nature of commercial networks means that reliable video transfer is not possible, reducing ability to decide upon evacuation in real time, and higher risk to deployed resources	Capture and transfer of building information and images in real time deliver more efficient decision making, better resource deployment and safer working environment for fire fighters
Large international finance summit	Relies on common operating picture being established between mobile command centre at the venue and central control rooms – this requires exchange of a range of information (voice, images, video) that are beyond the capabilities of existing dedicated networks	Transfer of sensitive personal data (e.g. iris or facial recognition) is not possible using a non-secure commercial networks. Requirement for high quality imaging applications to be available inside the venue also limits usefulness of commercial networks that do not always provide the necessary depth of indoor coverage	Capture and transfer of video and images in real time delivers a common operating picture, enabling more efficient decision making, better resource deployment and safer working environment for the summit

6.2 Limitations of upgrading commercial networks for future public safety services

As indicated in the section above, new mobile broadband services to meet future public safety user requirements could, in theory, be provided by upgrading commercial networks and engineering the deployment of these to achieve the specific operational requirements of the public safety sector. However, the consensus of the various reviewed documents is that there are a number of critical limitations inherent in using commercial networks for public safety applications, due to the core operational requirements that public safety communications need to meet.

While in theory it might be possible to upgrade and engineer commercial networks to meet these operational requirements (i.e. build new, shared, LTE networks that are engineered to meet both public safety and commercial user requirements), the balance of evidence in the reviewed documents suggests that this will be unachievable in practice. In particular, there are a number of reasons why commercial operators might be unwilling to make the necessary network changes to support public safety operational needs:

- the public safety sector requires very extensive geographic coverage as well as in-depth coverage penetration inside buildings, irrespective of location, which does not match the typical roll-out requirements of a commercial network
- it is likely to be very expensive to re-engineer commercial networks to achieve all of the public safety sector's operational requirements, and there are questions about whether sufficient incentives exist for commercial operators to do this. For example, typically requirements include the need for battery back-up to be available at thousands of base station sites across the network, and for networks to be designed to ensure that no single 'point of failure' exists either in access or core networks
- even if re-engineering costs are borne by the public sector, there is a risk that the resulting network will then be over-provisioned for commercial use. As such, commercial operators might find themselves having to pass additional costs (e.g. for the ongoing operation and maintenance of the network) on to commercial user tariffs, which is not viable given the competitive nature of the commercial mobile market. As such, commercial operators may not be willing to take on such requirements, given the potential risk to their commercial business
- there are questions about whether some of the public safety requirements are actually achievable. For example, to obtain the necessary layers of redundancy and prioritised access to capacity in urban areas might not be possible (since demand for capacity will also be high from commercial users, and hence reserving capacity specifically for public safety users might not be viable)[13]

[13] Furthermore, if the public users of the network know that in times of a local emergency they will lose the network services, this creates a disincentive for users to subscribe to that network, a risk that commercial operators are unlikely to take on.

- there is a question about whether the required Grade of Service for public safety use can be guaranteed within a network shared with commercial users, particularly in times of very high traffic loading
- there are conflicting views on whether signalling could be encrypted over the air interface in 3G/LTE
- ensuring the specific requirements for carriage of 'restricted' or 'confidential' documents requires careful network planning and approvals, which is complex and costly to achieve
- in conditions of local or national emergency, public networks typically become overloaded as the normal customer base seeks to communicate at the same time, and it is not clear that networks can be dimensioned to achieve the required immediacy and guaranteed access that public safety requires.

A further range of reasons why public safety users have been reluctant to make more widespread use of existing commercial networks, and have favoured the development of their own dedicated networks, are included in the various documents we have reviewed for this study. These include the points summarised below.

Coverage	Commercial operators typically invest in coverage where populations exist, and capacity is designed to maximise revenue generation in those areas, with little incentive to invest in areas of low-density population. Public safety, by contrast, requires ubiquitous coverage across a country's geography for everyday use, irrespective of population densities.
Network design	Re-engineering of commercial networks to meet public safety's requirements might be feasible in theory, but in practice would result in large parts of the commercial network being heavily over-engineered. This is likely to be more costly for the public sector to fund than a dedicated network provisioned to meet the specific coverage and capacity needs of the public safety user based, without having to provision for additional commercial traffic.
Sabotage	There is a view that commercial networks might be more vulnerable to sabotage by criminals that dedicated networks are, if the network is known to be used for public safety communications. Dedicated public safety networks are typically more guarded against sabotage through a range of specific measures e.g. vetted staff, secure fencing at sites, and networks designed to ensure no single point of failure in the event of sabotage, etc.).
Roll-out schedules	There are precise requirements for the roll-out of public safety networks (e.g. the need to align with police/fire/ambulance area boundaries), which do not match typical commercial roll-out strategies.
Risks of shared use	There are risks such as information security, quality of service and control of service level agreements if public safety users share networks with commercial users, which previous experience suggests can be avoided through use of dedicated networks under government control and supervision.
Reliance on commercial operators	There is a reluctance for public bodies to be reliant on a fully commercial operator, in view of the potential lack of control upon future network investment, business plans and financing.

If the upgrading and engineering of commercial mobile broadband networks is not feasible to meet public safety requirements, as this section suggests, the only alternative is to develop a new generation of dedicated mobile broadband networks designed to meet specific public safety requirements. For this to be achievable, additional spectrum will be required.

7 Conclusions

The study has found that, in line with societal trends evident within today's Information Society, a diverse range of data, imaging and multimedia applications are in demand within the public safety sector. Demand for access to a wider range of information is being driven by changes in working practices, which is creating requirements for access to a far wider range of data sources (textual, images and video) that are typical in commercial mobile networks. Sharing of various data types (textual, images, video, etc.) is being used in order to establish and maintain a common operational picture between agencies and between field and central command staff. This is being used to improve responsiveness, aid the deployment of resources, and improve timeliness and decision making in daily public safety operations and when responding to major planned or unplanned events.

Three of the four evolutionary paths developed for this study illustrate the public safety sector's need for a next generation of mobile broadband networks to deliver the range of applications that are envisaged in the future. As there is a limit to the range and volume of data and multimedia applications that existing dedicated narrowband and wideband networks, and existing commercial networks, can provide, if a new generation of mobile broadband networks is not made available, some new applications cannot be delivered. Ultimately, this will affect how already emerging changes to ways of working within the public safety might evolve, and, in the longer term, constrain the further development of the sector.

A new generation of services could in theory be delivered using an upgraded commercial network (e.g. HSPA/HSPA+ or LTE) with network deployment engineered to meet specific public safety requirements. However, as explained in Section 6.2, this option does not appear to be achievable in practice. The only other option is therefore to encourage industry to develop a new generation of mobile broadband networks for dedicated public safety use.

To enable the industry to devote the necessary investment to develop new dedicated networks, there is a need for additional spectrum to be identified, since existing bands are already fully utilised to deliver existing public safety systems.

It should be noted that identifying suitable spectrum is on the "critical path" to support development of a new generation of dedicated mission critical mobile broadband solution, because of the timescales associated with identifying suitable spectrum.

The requirements for additional spectrum are based upon the combination of the various factors identified throughout this report, specifically:

- trends in the range of data and multimedia applications in demand within the public safety sector
- potential increase in user densities and intensity of use for data applications

- specific traffic characteristics of public safety operations (e.g. network-centric ways of working)

- the infrastructure and technical requirements to meet the operational requirements of the public safety community (e.g. availability, security, reliability, latency), and limitations in use of commercial networks to deliver these.

Given the cost of deploying new networks, access to spectrum in bands below 1GHz will ensure maximum commonality with existing dedicated networks deployed in the 380–385/390–395MHz bands, facilitate re-use of assets where possible (e.g. radio sites). Use of spectrum above 1GHz (e.g. around 2 GHz) might be feasible, but would incur significantly higher roll-out costs compared to that below 1GHz, raising questions at national government level as to whether and how the additional costs can be funded.

Based on the reviewed documents, the European dimension to the public safety spectrum requirement is important for a number of reasons:

- the public safety sector is a niche market and therefore benefits from the identification of harmonised spectrum even more than other mobile systems (e.g. GSM or UMTS), because of the smaller user base and resulting lower volumes of equipment and terminals

- even if commercial solutions are adapted to meet specific requirements of a niche sector such as public safety, there are still costs involved in the necessary modifications, and therefore harmonised spectrum availability is key to ensure that manufacturers are able to develop products for a European market. An example of the re-engineering of existing commercial standards to meet niche requirements is that of GSM-R (the railways version of GSM) – although the GSM standard is supported by all major vendors around the world, GSM-R equipment is supplied by relatively few and the availability of harmonised spectrum for the product has therefore been important to reduce costs

- interoperability is an increasingly important requirement within the public safety sector, both to communicate between different public safety authorities within a country, and to communicate across borders. This is evidenced by a number of the documents reviewed for this study. [14]

The lack of available spectrum is therefore a significant barrier to the further development of mobile communications capabilities tailored to meet public safety requirements, until such time as a new, harmonised band can be identified at a European level.

[14] For example, Council of the European Union, Draft Council Recommendation on improving radio communication between operational units in border areas

Annex A: List of acronyms

ANPR	Automatic number plate recognition
AVL	Automatic vehicle location
CEPT	European Conference of Postal and Telecommunications Administrations
ETSI	European Telecommunications Standards Institute
GHz	Gigahertz, 1GHz is equal to 10^9 hertz
GIS	Geographic information system
GPRS	General packet radio service
GSM	Global System for Mobile Communications, the most prevalent international standard for second-generation cellular mobile systems
GSM-R	GSM-Railway, an adapted version of the GSM standard used by Network Rail (UK) and other railway authorities in Europe to provide train-to-track signalling
HSPA(+)	High Speed Packet Access, a protocol that can form an overlay to existing 3G networks to speed up network capacity and transmission rates
ITU	International Telecommunication Union
LTE	Long Term Evolution, the next generation of 3GPP standard, which uses an OFDM radio interface – sometimes referred to as “4G”
MHz	Megahertz, 1MHz is equal to 10^6 hertz
NATO	North Atlantic Treaty Organization, the military alliance of countries in Europe and the USA
OFDM	Orthogonal frequency-division multiplexing, the air interface that is used in WiMAX systems and will be used in LTE
PABX	Private automatic branch exchange, a telephone exchange serving a particular business/office
PBR	Private Business Radio, generic term used to describe the variety of two-way, self-provided, mobile radio systems used by a variety of business users in Europe (including airports, taxi firms, local authorities and the Emergency Services pre-Airwave analogue radio systems)
PSTN	Public switched telephone network
RFID	Radio frequency identification
TEDS	TETRA Enhanced Data Service
TETRA	Terrestrial Trunked Radio, the digital trunked radio standard used by the Airwave service in the UK and in other Emergency Services mobile radio systems in a number of other countries Europe and around the world
UHF	Ultra high frequency, i.e. between 300MHz and 3000MHz
UMTS	Universal Mobile Telecommunications System, the European standard for third-generation cellular mobile systems
VHF	Very high frequency, i.e. between 30MHz and 300 MHz
WCDMA	Wideband CDMA, the technology used in current 3G systems
WiMAX	Worldwide Interoperability for Microwave Access, the technology forming the IEEE802.16e wireless broadband
WGFM	Working Group FM
WRC	World Radiocommunication Conference, the international conference held by the ITU every few years to update the international frequency allocation table
3G	Third-generation mobile systems
3GPP	3rd Generation Partnership Project, a partnership between ETSI and standards bodies in the USA and Asia, responsible for developing industry equipment standards for 3G systems

Annex B: List of documents reviewed for this study

This annex contains a list of the selection of documents from a range of public-domain sources, which have been reviewed for the study.

No.	*Document reference*	*Document title*	*Author*	*Version*	*Publication date*
1	Results from last TC-Tetra workshop in Brussels	TETRA Association Future Vision workshop held in Brussels on 25th February 2009	Various	-	February 2009
2	Results from previous TETRA Association workshops on mobile data [*two workshops*]	a. TETRA Association Applications workshop in London (December 2009) and mobile data applications questionnaire b. TETRA Association TEDS workshop (March 2007) and TWC questionnaire (2008)	Various	-	December 2009 / March 2007
3	Results of Analysys Mason study	Exploiting the digital dividend – a European approach	Analysys Mason	Final report	14 August 2009
4	PCWG ad-hoc group studies	Police Cooperation Working Group – Improving radio communication between operational police units in border areas; analysis of the responses received to the data capture exercise on cross border working	Police cooperation working group	-	December 2008 16 March 2009
5	ETSI System Reference Document on future Public Safety and Security (PSS) Systems	TR 102 628: System Reference Document; Land Mobile; Additional spectrum requirements for future Public Safety and Security (PSS) wireless communications systems in the UHF range	ETSI	V1.1.1	10 June 2009
6	Results from ERO questionnaire on PPDR	FM38(09)15 Rev 2 Annex 3, Result of Questionnaire on PPDR	ERO summary in response to CEPT WGFM PT38	Rev 2	April 2009
7	Results from TC-RSS WG4 questionnaire	RRS08_018_ETSI_TR_102_733 and TR 102 734 (Aug draft)	ETSI	V0.0.12	November 2009
8	Results from the expert group on police cooperation	Draft Council Recommendation on improving radio communication between operational units in border areas	Council of the European Union	Draft	20 May 2009
9	Document from MESA	Project MESA; Service Specification Group - Services and Applications; Statement of Requirements (SoR)	MESA	V3.3.1	March 2008
10	EU-TOIA report on digital dividend	Extract: Toia Report on Digital Dividend/2008-09-26 - Text adopted	Rapporteur - Patrizia Toia	P6_TA-PROV(2008)09-24	24 September 2008
11	WIK study	Safety first – Reinvesting the digital dividend in safeguarding citizens	Kenneth R. Carter and Val Jervis	-	5 May 2008

12	PSC-Europe response to digital dividend	PSC Europe response to the digital dividend hearing	PSC Europe	-	11 June 2008
13	EULER End User Requirement	EULER End User Requirements Deliverable 2.3-1	Dimitrios Symeonidis	V0.8	17 September 2009
14	TETRA Association Spectrum Group study	What data service will the future bring – from a TETRA perspective	TETRA Association Spectrum Group	Draft	November 2009
15	Wireless broadband study by Public Safety Spectrum Trust Chairman, Harlin McEwen	Public Safety Radio Communications; Wireless Broadband is not an alternative to LMR mission critical voice systems	Chief Harlin R. McEwen	Draft	12 October 2009
16	Hansard Report	Column 761	Lord Lucas	-	2 December 2009
17	Safecom document	Public Safety Statement of Requirements for Communications and Interoperability	US Department of Homeland Security	Volume II Version 1.2	August 2008
18	Westminster e-Forum	Westminster e-Forum keynote seminar, Emergency Services and Public Safety Spectrum	Westminster e-Forum	Transcript of event	11 June 2009
19	PSC Europe white paper	Public safety first	Jeppe Jepsen	-	-
20	Report for BAPCO	The “Business Case” for Blue Light Spectrum	David Happy	-	26 August 2009

Annex C: Summary of document review

C.1 TETRA Association Future Vision Workshop (Brussels)

Item	*Description*
Document title	TETRA Association Future Vision workshop held in Brussels on 25th February 2009
Author	Various
Publication date	February 2009
Abstract	Various presentations discussing the future vision for TETRA towards a fully integrated ICT solution providing NB/WB/BB wireless communications for "mission-critical" and traditional PMR/PAMR applications, through the enhancement and/or provision of user driven services and facilities and the utilisation of the latest in technology, innovations and standards. The workshop discussed applications including data rate, bandwidth and QoS, user requirements for broadband data, and other areas of consideration in the selection and standardisation of a broadband solution.
Requirements or needs identified in report	The need for the industry to evolve TETRA towards a fully-integrated seamless ICT solution providing NB/WB/BB wireless communications for mission-critical and traditional PMR/PAMR applications. Data and image applications are emerging as a strongly needed requirement to improve users' efficiency and safety. The fundamental requirements are: • Ability to communicate in all locations (100% radio coverage) • Instant access at all times (perfect Grade of Service) • Never goes wrong (100% reliability) • Voice and data (V+D) communications • Perfect voice quality in all operational environments (ability to recognise who is talking) • Ability to support all V+D applications • Private and secure communications when required • RF coverage in black spots and outside main network • Additional capacity when localised traffic demands are high • Fall-back communications if base station and/or network fails • Ability to support all non-voice applications (real-time and other) • Standardised technology solution providing: ▪ competition ▪ choice ▪ second source security • Interoperability: ▪ within the same organisation ▪ within other related organisations as required (e.g. police, fire, ambulance, military, transport, utility, etc.)

- cross-border with other nations as required
- Interworking with other technologies as need (Public Networks, 3G, etc.)
- Evolution:
  - backward compatibility
  - maximum reuse of existing infrastructures
  - future proof
  - enhancement
  - integrated and seamless ICT
- Current mission-critical communication needs to be:
  - dedicated
  - wide-area
  - secure
  - reliable
  - available
  - fit for purpose.

Possible applications identified in report

Real-time applications, where source generates the information to the destination and strict constraint to delay and its variation over the network is fundamental for using the application.

Non-real time applications, where the source has the information and sends it to the destination. Source can send part of the information missing and re-order the packets.

Applications include:

- Automatic stolen car plate recognition (approx 10byte/plate required throughput)
- Biometric check
  - fingerprint required throughput per officer – check rate: 8 people/min
  - γ=(8people/min) / (60sec/min) x 1kByte/People =133byte/sec = 1.06kbit/s
- Image transmissions
  - target acceptable resolution: dimension 20kByte = 160kbit/ user
- Face recognition
  - the minimum number of pixels to recognize faces is 40PPF (pixels per foot) the minimum number for reading license plates is 80PPF
- Mobile office
- Database queries
- Video surveillance from the field
- Mobile command centre sharing an accurate situation picture of an incident
- Delivering images, maps and floor plans to the field
- Detailed ECG traces from ambulance to hospital and other telemedicine applications
- Fingerprint identification/authentication
- Image/audio capture
- Geographical positioning

	• Electronic identity document reading • Voice communications • Data connectivity • Optical character recognition (OCR) • Electronic signature certificate management • Cryptography
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	Not applicable
Possible scenarios identified	Not applicable

Any other relevant information from the report	Possible TEDS broadband solution:
	• Integration of other technologies with TETRA
	  ▪ Use of TETRA 2 infrastructure as the core network
	  ▪ 3G technologies such as HSPA, LTE or EV-DO, UMB
	  ▪ WiMAX (preferably narrowest channel options at lowest designated WiMAX frequencies)
	• TEDS Technology Evolution
	  ▪ Use of wider carriers than TEDS
	  ▪ More spectral efficient channels
	  ▪ Other features under discussion in WG4
	  ▪ Acquisition of new spectrum for interoperable TETRA 2 (plus BB enhancement) networks?
	• Other comparative considerations
	  ▪ LTE, WiMAX and other public BB networks designed for mass market/urban applications
	  ▪ Wider and wider carriers, smaller and smaller footprints
	  ▪ Design criteria: capacity limited, maximum commercial return
	  ▪ No slack capacity for emergency communications
	  ▪ PPDR networks design criteria: coverage limited
	  ▪ Full national coverage essential for PPDR; capacity is not an issue
	  ▪ Narrowest bandwidth/lowest frequency band compatible with required PPDR applications and spectrum availability
	  ▪ NB, WB and BB in the same frequency band
	  ▪ PMR type security, availability and reliability
	• Operational use for video must be understood
	  ▪ What is required in a court case (used as evidence)?
	  ▪ What is required in emergency response?
	  ▪ What is required for surveillance, facial, licence plate recognition?

C.2a TETRA Association Applications Workshop and mobile data questionnaire

Item	*Description*
Document title	TETRA Association Applications workshop held in London on 2nd December 2009 Mobile data applications questionnaire results
Author	Various
Publication date	December 2009
Abstract	Various presentation discussing applications for TETRA.

Requirements or needs identified in report	Security, safety, cost and service are the critical features of an optimal mission-critical data solution, along with a requirement for an integrated system that can be used throughout the response chain (i.e. services all accessible via the same terminal or device) and data services as reliable as TETRA voice.
	Customer specific applications that enhance the functionality or usability, versatility and productivity of the TETRA radio terminal for different purposes.
	Existing applications require more capacity.
	Ability to move office applications into the field.
	Operational needs: resilience; availability; security.
	• Ciphering and encryption
	• Mission critical communication
	• Availability of resources under all circumstances
	  ▪ operational even when public networks are congested
	• Resilience
	  ▪ ability to work in crisis situation (major electrical disruption, transmission network failures, etc.)
	• When all public communication infrastructure are out of order, the radiocommunications network should be kept operational.

Possible applications identified in report	Current applications:
	• Collect and share common situation picture
	• Allocate right resources efficiently
	• Distribute and obtain information instantly
	• Collect surveillance, medical, etc. monitoring information
	• Automate administrative routines
	Future applications:
	• Fingerprint recognition
	• Licence plate recognition
	• e-Passport reader
	• RFID reader
	• JAVA applications on TETRA terminals:
	  ▪ Access information in remote databases
	  o Vehicle databases
	  o Criminal records
	  o Hazardous materials

	▪ Report location–related information o Task progress o Intelligence information o Support requests ▪ Push images to field officers o Suspects from surveillance camera o Missing persons o High risk suspects • Streaming video ▪ Transmission of live videos simultaneously to/from the central command and field personnel ▪ Relaying ad-hoc videos and surveillance camera to the central command and field personnel ▪ Air-to-ground video • Real-time collection of large medical data ▪ Sending full data on a patient's condition from the ambulance ▪ Remote surveillance of smoke divers' vital functions ▪ Remote surveillance of patrolling officers' vital functions • Access to geographic images ▪ Aerial photographs ▪ Satellite images and maps ▪ Plans of buildings • Remote database queries for passport and biometric details • Sending photographs of lost children and wanted people • Access too the Fire service 'Gazetteer' for information on HazMats on premises • Transmission of live video to and from the central command and field personnel • Relaying ad-hoc video and surveillance camera • Sending full data on patient's conditions from the ambulance • Integrated broadband data services which are emerging as an important PSS need require more bandwidth – ideally two paired 15MHz channel • Telemedicine • Extensive geo-location capabilities • Web applications • Full email • Over-the-air downloads for software upgrades
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	There are network availability issues with commercial networks, for example: • Motorway Car Crash – statistics show that the network call volumes increase during a major auto crash. People involved call loved ones, witnesses call for assistance and other drivers call to say that they will be late. What is the impact to data?

	• Major Sport Events – peak GSM/GPRS load times are before, half time and after the match = critical times for secured communications. Historically mobile telephony calls can fail during these periods
	• Natural disasters and terrorism – after the Madrid bombings; the mobile phone network collapsed at 8:05am and was out of use for eight hours
	• Public networks do not meet PS user requirements
	  ▪ Coverage, Availability, Security, Resilience, Interoperability
	  ▪ Control, Functionality
	• Public network operators are able to prioritise PS users, but
	  ▪ When the public is cut off, they call the emergency services to get information.

Possible scenarios identified	Not applicable

Any other relevant information from the report	• Mission critical applications can be optimised to reduce the amount of data that is transmitted over lower bandwidth wireless networks: the communication payload:
	  ▪ TCP/IP – 40bytes
	  ▪ UDP/IP – 28bytes
	  ▪ Radio optimised TCP/IP – 10 to 15bytes
	• Mobile data helps effectively to:
	  ▪ Collect and share common situation picture
	  ▪ Allocate right resources efficiently
	  ▪ Distribute and obtain information instantly
	  ▪ Collect surveillance, medical etc monitoring information
	  ▪ Automate administrative routines.

C.2b TETRA Association TEDS workshop and TWC survey

Item	*Description*
Document title	TETRA Association TEDS workshop held in Bonn on 27th March 2007 TWC questionnaire in 2008
Author	Various
Publication date	March 2007
Abstract	Various presentations discussing user requirements, technical specifications for TEDS, spectrum and regulatory issues and applications for TEDS.
Requirements or needs identified in report	There is a need for mission critical data and data speeds beyond the TETRA 1 narrow band service. The capacity enhancements brought by TEDS are also needed so that systems can handle the load of multiple, concurrent narrow band data services such as database access and ID-card or fingerprint verification. The usage scenario in the field seems to be developing towards a network-centric way of working that relies on personalised data and where an overview of the incident is shared, which improves the situational awareness. More and more daily routines are expected to move to take advantage of data and there is a trend towards mobile offices – activities traditionally confined to an office environment are possible in the field. Need for the “higher bit rates” in wider channels: • Higher bit rates (150–500kbit/s?) • Wider channels (150kHz?) • Spectrum (2×5–10MHz?) • Timing TIP certified product available: 2010? Need for TEDS spectrum in PSS (based on re-use factor of 20 or more): • One 50kHz layer ▪ 2×20×50kHz = 2×1MHz absolute minimum ▪ 2×30×50kHz = 2×1.5MHz reasonable minimum • Double 50kHz layer (100kHz per site) ▪ 2×20×100kHz = 2×2MHz absolute minimum ▪ 2×30×100kHz = 2×3MHz reasonable minimum Applications need to work on multiple networks to maximise available coverage area and bandwidth Key Nødnett (Norwegian PS Network) TEDS User Requirements: • Basic user requirement is for the transfer of 100KB of data (e.g. picture) from a radio terminal within 10 seconds • No specific data applications identified at this stage but rather the expectation that there will be a strong operational need for higher speed data applications in the future • TEDS upgrade must minimise any disruption to the ’live’ network • Level of encryption must be at least as good as TETRA 1
Possible applications identified in report	• Personalised information • Mobile command and control – dispatching • TEDS as data only layer – voice services provided by TETRA 1

	• Location tracking
	• Narrow band services
	  ▪ Scanned images (ID-cards) for verification
	  ▪ Database access
	• Wide band services
	  ▪ Video, both uplink and downlink
	  ▪ Messaging including attachments
	  ▪ Maps and drawings, images to vehicles
	  ▪ Remote maintenance – download of terminal configuration, firmware, software
	Top TEDS data applications identified at workshop:
	• Navigation / location tracking / AVL
	• Database queries (medical journal lookup, simple query and image-query)
	• High resolution still pictures (pictures from field, maps, fingerprint, vital data sampling)
	• Instant Messaging / email / news (field-to-field and office-to-field)
	• Electronic forms (paperwork, ambulance, home nurse)
	• Telemetry (sensors in vehicle / on patient)
	• Web browsing
	• Video streaming (surveillance) and video conferencing

Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	No, as commercial data services cannot be expected to be available at all times.
Possible scenarios identified	Not applicable

Any other relevant information from the report	TEDS features:
	• To be included in the TEDS TIP:
	  ▪ Security
	  ▪ Modulation 4/16/64 QAM
	  ▪ Service interaction
	  o Voice services offered to user busy in TEDS data service
	  o Concurrent voice and data
	  ▪ Quality of Service
	  ▪ TEDS PEI (MEX)
	  ▪ Multi-slot operation
	  ▪ Sectored cells (extended coverage)
	  ▪ High speed
	• Additional TEDS Features which would first need standard update:
	  ▪ Multicast
	• Devices:
	  ▪ Data only TEDS devices
	  ▪ Mobile and hand portable TEDS enabled voice & data devices
	TEDS does not cause significant interference to other systems but TEDS cannot co-exist with military air-ground-air radios.

C.3 Analysys Mason study on digital dividend

Item	*Description*
Document title	Exploiting the digital dividend – a European approach
Author	Analysys Mason, DotEcon and Hogan & Hartson LLP
Publication date	14th August 2009 (Final report)
Abstract	This document summarises the work carried out on behalf of the Information Society and Media Directorate General of the European Commission to ascertain what action needs to be undertaken at EU level to ensure the benefits of the digital dividend are maximised, including: • conducting an inventory of the situation in each Member State regarding the digital dividend • carrying out analysis to understand the demand for the spectrum as well as the social and economic value of potential users • reviewing technical issues, such as technology trends, interference issues • developing a range of scenarios for a co-ordinated EU approach, and a cost/benefit analysis of each approach. The report identifies seven potential uses of the digital dividend – DTT, commercial wireless broadband, services ancillary to broadcasting and programme making (SAB/SAP), broadcast mobile TV, cognitive technologies, wireless broadband for public protection and disaster relief (PPDR) and an innovation reserve. The study offered a set of recommended actions for a co-ordinated approach and a proposed roadmap for implementation.
Requirements or needs identified in report	The need for high bandwidth wireless services. PPDR is widely perceived as a high-value use of spectrum and the value of this use cannot be expressed solely in economic terms, as PPDR systems are used for safety of life and are regarded as necessary government services.
Possible applications identified in report	High-speed data transfer, e.g. paramedics need to transmit medical images and or reports to colleagues ahead of their arrival at the hospital. Real-time video transmission, e.g. to improve efficiency; ability to see what is happening at the scene; and instantly collaborate with central command, co-workers and other agencies.
Possible benefits identified in report	A PPDR network would be a key asset in the development of public health services and security for all, and as such would sustain the quality of life of citizens across Europe.
Can the benefits be realised using commercial networks	Commercially available wireless broadband technologies (e.g. WiMAX and LTE) could offer economies of scale and superior handset availability but may not be sufficiently reliable as they are optimised for different objectives than PPDR.
Possible scenarios identified	Not applicable
Any other relevant information from the report	The emergency services rely on good in-building coverage in order to communicate effectively at the scenes of incidents, and so spectrum below 1GHz is particularly suited to meet their requirements. In its 2008 Communication on “Reinforcing the Union’s Disaster Response Capacity” , the Commission stated that “European citizens expect the Union to protect their lives and assets inside the EU” and stated that the “challenge of disaster prevention, mitigation and response…require[s] a comprehensive

approach by the EU to the continuum of disaster risk assessment, forecast, prevention, preparedness and mitigation (pre- and post-disaster), bringing together the different policies, instruments and services available to the Community and Member States working as a team".

Wireless broadband for PPDR (in addition to or to replace existing services) could realistically only be deployed terrestrially using spectrum below 1GHz, deployment at high frequencies would be too costly. It may be possible to deploy such a service in other bands, such as 450MHz, but less spectrum is available and it would require concerted coordination across Member States. Thus the incremental value is either (a) the additional value over and above existing national services; or (b) any extra costs or changes in service quality from using another band.

C.4 PCWG ad-hoc group studies

Item	*Description*
Document title	Police Cooperation Working Group – Improving radio communication between operational police units in border areas; analysis of the responses received to the data capture exercise on cross border working
Author	Police cooperation working group
Version	-
Abstract	Based on two documents – responses from 12 administrations to a questionnaire sent out on cross border working and a technical brief discussing the medium and long term goals for cross border emergency services mobile communications requirements following the survey. The Police Cooperation Working Group created a technical ad-hoc expert group on the future of radio-communications in July 2008, following the EURACOM seminar whose main objective is to identify technical solutions to foster interoperability between police forces, especially in border areas. The document puts together some ideas of how interoperability and cross border communications might be accomplished at a technical level and discusses a number of the issues that arise. The questionnaire addresses the requirements for voice, data, coverage, encryption requirements, spectrum and consideration of using a public network. The outcome of a three country pilot experiment in cross border communications was carried out between Germany, Belgium and the Netherlands was also presented.
Requirements or needs identified in report	• Full interoperability across Europe • Ability to create talk groups across networks • Pan-Europe direct mode capability • Ability to handle biometrics and other imagery and video-mobile broadband capability • Access to both home and local databases (this must be managed carefully with respect to security issues) • End-to-end encryption is preferred but air interface only encryption is accepted by some administrations • Full area seamless communications / interoperability across Europe (ISI?) • Border zone coverage, approx 15km • Access to both home and local control rooms (language issues will be highly significant and may be a greater obstacle than the technical issues) • Ability to create talk groups including home and visiting officers (patch functions) • Point to point calls and telephone interconnect • Automatic location capability for persons and vehicles and assets • Access to home databases and local databases for visiting officers including biometric databases • Harmonised spectrum – spectrum for mobile broadband minimum 2×10MHz, more realistic to look for 2×16MHz. Harmonised spectrum is key to providing full access across borders.
Possible applications	Voice

identified in report	• Full communications with home control room • Access to local force communications control room • Group based communications Data • Biometry • Video (on-line streaming) from field officer • Video (on-line streaming) to field officer • GPS position location information • Database access • Transmission of patient data, maps, building drawings • Others including SDS, SMS, status messaging, situational awareness and common picture functionality
Possible benefits identified in report	More successful and efficient cross border inter-working.
Can the benefits be realised using commercial networks	All the responses provided a consensus that public networks including GSM, 3G, etc. can be used as a backup to dedicated service and for non-critical traffic only.
Possible scenarios identified	Not applicable
Any other relevant information from the report	For a cross border mobile broadband capability European harmonised radio spectrum is an absolute requirement, as it has been for the current voice communications capability. This point needs to be clearly understood and communicated to spectrum management administrations. Failure to achieve harmonised spectrum will remove the possibility for secure and resilient cross border mobile broadband communications for the foreseeable future. A much more difficult situation is cross border communications between TETRA and TETRAPOL networks. Since TETRA is a TDMA based technology and TETRAPOL is based on FDMA the two air interfaces are physically incompatible. There would therefore be limited benefit in the development of an ISI. TETRA networks mainly provide emergency mobile communications in Europe, but there are also some TETRAPOL systems. Most operate at or close to 380/400MHz. Given the difficulties noted above it likely that full successful interoperability will only be achieved across Europe when all the participating countries are: • using a common air interface standard for voice and data • operate a minimum defined set of network features • have deployed a set of agreed configuration parameters • operating in a common frequency band. There is a requirement for the following: emergency call, individual call, group call with units on both sides of a border, duplex individual calls to telephone networks (telephone interconnect), fast set up for group and point to point calls. As countries develop their mobile communications services new technologies are likely to be introduced. The UK is in the process of commissioning the Future Communications Programme (FCP) to replace the Airwave TETRA network for both voice and data communications. No decision has yet been made on the technology to be deployed. FCP will start to enter service from 2014. Cross border issues will need to be considered from the outset of the commissioning process for new networks.

Full interoperability should imply access to local control rooms and the ability to create talk-groups across networks. Effectively this suggests the formation of a super network of interconnected networks. Thought needs to be given to the creation of a standard feature set and the management of this super network capability including issues of confidentiality and national security.

A three country pilot experiment in cross border communications was carried out between Germany, Belgium and the Netherlands. The outcome:

- Four pilot groups were available however, it was not possible to select a national group in a foreign network and it was not possible to indicate which network the terminal was registered
- Emergency calls were transferred to the selected (international) group and audio could be heard by all dispatchers and radios in the three networks within this selected group
- Emergency call signalling was only possible in the network in which the call was initiated, signalling was not transferred to the other networks.
- Possible to make an individual call to another radio when both radios were registered in the same network. The reason for this is that signalling was not being transferred to the other foreign networks.
- Telephone call was supported, however the set up of a telephone call was different for each network.
- Fleetmap – each subscriber that wanted to migrate to another network needed to have a unique ITSI that was not used in the foreign network. In other words, the ITSI needed to be known and equal in all three networks. This was similar for groups and the corresponding GSSI's.

C.5 ETSI SRD on Public Safety and Security (PSS) Systems

Item	*Description*
Document title	TR 102 628 – System Reference Document; Land Mobile Service; Additional spectrum requirements for future Public Safety and Security wireless communications systems in the UHF range
Author	ETSI
Version	V1.1.1 (2009)
Abstract	This document describes the spectrum requirements of future PSS communications for wideband and broadband applications. The document refers to narrowband and wideband PPDR applications in Europe being covered by TETRA Release 1 and TETRA Release 2 (TEDS), but that there is a need for interoperable, secure and wide-area communications for public safety users for wideband and broadband applications. This cannot be accommodated in existing spectrum available to PSS users since that spectrum is already fully used by voice traffic and some data usage. The document summarises spectrum requirements of 2 separate contiguous blocks of 10 MHz plus two separate non-contiguous blocks of 6 MHz dedicated to PSS and harmonised across Europe; the total of 16 MHz for each direction to fit within a tuning range. The required frequency range is between 300 MHz and 862 MHz, preferably in the lower parts of the band. The document advocates allocation of a dedicated spectrum band for harmonised wide-area communications capable of high-speed IP based data applications. Spectrum should be sufficient to meet the requirements of day-to-day PSS traffic and also cater for peak usage during major incidents
Requirements or needs identified in report	• Mission critical PPDR communications are exhibiting an urgent and growing need for inter-operable high-speed data services. • The wideband ECC Decision for 380-470 MHz does not give the PPDR community extra data capability, since the actual spectrum available is insufficient to accommodate high speed data applications • Lack of further availability of spectrum will risk the future development of the PPDR community through inability to support new services requiring more data (e.g. identify cards, photographs, fingerprints), failing to keep pace with societal developments where society is increasingly adopting advanced data applications, and inability to manage major disaster scenarios efficiently • User communities have determined that mobile data is equally as missions critical as voice, and therefore cannot be safety transported over commercial mobile networks. This is because officers will become more and more reliant and dependent on mobile data communications in support of their day-to-day operations • PSS TETRA networks will start being replaced, at least in part, from around 2012 onwards, with new technology needed to support voice, narrowband, wideband and broadband data services and be backward compatible and interoperable with existing (TETRA) networks • Spectrum requirement includes one contiguous component of at least one broadband channel width (10 MHz). Split of spectrum or fragmented spectrum is not viable due to RF front end complexities and difficulties with interoperability • Specific public safety operational requirements include control over security implementation and other operational aspects of the network, redundancy of components on cell sites (e.g. transceivers, site controllers, antennas), redundancy of UPS power supply capability,

	including battery and generator powered supplies, a high degree of network resilience (e.g. overlapping coverage from multiple cell sites), fallback strategies to allow stand-alone operation of sites disconnected from the rest of the network, redundant switching and a high level of RF coverage • DMO is required in all radio terminals, plus availability of the associated repeaters and gateways to provide RF coverage in difficult areas or where base station coverage has been lost • Need for fast communications set-up in combination with a much higher call set-up success rate, typically 99% or even higher for PSS compared to what is offered by public networks
Possible applications identified in report	• At present, operational PSS networks support voice and narrowband data services only. Whilst those applications will continue to be required, others that are needed include video conferencing, video streaming, full satellite navigation, secure passport and bio-metric checks, online access to various databases, full email internet browsing, and improved transfer of files (including maps and pictures) • Ability to move the back office into the field • Sending detailed photographic images of lost or wanted people • Relaying ad-hoc video camera and surveillance camera real time information to patrol cars • Sending detailed maps and plans • Sending biometric data from an incident in real time, rather than having to return to the office • The ability to transfer video data back to incident commanders to make faster and more informed decisions • Cross-departmental communications • References data service attributes from ETSI TS 102 181 of email, imaging, digital mapping, location services, real time video, slow scan video, remote database access, database replication and personnel monitoring
Possible benefits identified in report	• Socio-economic benefits include: saving lives of citizens and public safety officers, minimising damage to properties, faster response, more efficient communications, enhancement of a single emergency communication network with high reliability, availability and security, better co-ordination between different public safety organisations and agencies both nationally and over borders • Potential to enhance investments in European national public safety infrastructures through evolutionary enhancement • Single wide-area coverage network resulting in major cost savings in the network infrastructure compared to use of multiple solutions • Creation of a pan-European or global harmonised set of equipment requirements, resulting in higher economies of scale and lower costs.
Can the benefits be realised using commercial networks	• The mandatory services and facilities required by public safety organisations can only partially be provided on networks designed for commercial use, since those networks cannot be used to carry mission critical traffic • In many commercial networks, data is sent at lower priority than voice, which could be a significant problem for public safety users who often find themselves in areas where voice services are being used intensively, but that data services are also needed

	• Even if a commercial network was designed to meet the operational needs of public safety users – i.e. resilience, QoS, security – many Governments would still need to ensure that ownership of the operator would be under Government control, or alternatively may require continued guaranteed financial viability and/or options to take management control of the network when needed
Possible scenarios identified	• Large fire encompassing 3-4 blocks in a large city or a large forest fire • Large public event e.g. Commonwealth Heads of Government Meeting, G8 Summit, Olympics • High-resolution video communications from wireless clip-on cameras to vehicle-mounted laptop used during traffic stop or response to other incidents, and video surveillance of security entry points such as airports with automatic detection based on reference images, hazardous materials or other relevant parameters • Remote monitoring of patients and remote real-time video view of the single patient
Any other relevant information from the report	• Annex A.2 refers to recent survey conducted by Motorola and APCO of more than 200 public safety administrators and officers in the top 100 US markets regarding current and future use of communications • Annex B.2 refers to technology evolution e.g. narrowband-wideband-broadband

C.6 Results of the questionnaire on PPDR prepared by ERO on behalf of CEPT WGFM PT38

Item	*Description*
Document title	FM38(09)15 Rev 2 Annex 3, Result of Questionnaire on Public Protection and Disaster Relief
Author	CEPT European Radiocommunications Office (ERO) on behalf of CEPT Working Group Frequency Management (FM), project team 38 (FM38), with responses from spectrum authorities, PSS users and industry
Version	Questionnaire issued February 2009, results April 2009 Contained in zipped file ERO_401925899884259
Abstract	The questionnaire was prepared by CEPT WG FM38 and issued to CEPT spectrum authorities/regulators to gather information concerning future mobile radio applications, and associated spectrum requirements, associated with Public Safety and Disaster Relief (PPDR) – also referred to as Public Safety and Security (PSS). Spectrum authorities that participate in the FM38 group were asked to forward the questionnaire to public safety users within their countries (i.e. police, fire and ambulance authorities) and invite them to respond to the questionnaire too. The questionnaire had two purposes (i) to collect information from users to clarify the user requirements and needs for mobile radio applications for PPDR (ii) to invite authorities/regulators to consider possibilities to identify additional spectrum for public safety use, and candidate bands below 1 GHz. 52 replies received – 23 from authorities/regulators, 19 from user organisations and 10 from industry.
Requirements or needs identified in report	Current applications will continue to be required in future, along with a range of new applications, with increasing emphasis on: • Broadband (e.g. real time video surveillance, including live CCTV images and images captured and relayed from helicopters) • Enhanced graphical data exchanges • On-site expert medical support • Situational awareness at fire incidents, to inform control/field decision making • Giving the officer in the field in charge of a major incident the same functions as an operator in the control room (“taking the control room out into the field”) • Remote situational assessment and control • Automatic facial recognition • Much higher data rates for database querying, geo-location etc. • Mobile office • Licence plate checks.
Possible applications identified in report	All present applications (listed in table below) also required in future, along with increasing emphasis on much higher data rates to improve efficiency of current applications, mobile control room, mobile office, video surveillance.
Possible benefits identified in report	1. Many of the companies who produce TETRA equipment are based in the UK and therefore the UK export market has benefited from the harmonised development of the TETRA standard 2. Vital for national security reasons

Can the benefits be realised using commercial networks	PSS users have specific operational requirements that public networks cannot deliver: • Resilience – overlapping cell coverage, redundancy of components, multiple backhaul links from individual radio sites, resilient switching (adjacent cells to be connected to different switches), fall back sites, power standby, etc. • Commercial networks do not offer professional radio oriented services (e.g. semi-duplex voice transmission for group calls, direct mode, different user priority levels and pre-emption) • Lack of security with commercial networks • In some countries there are limitations relating to the ownership/share structure of operating companies providing secure Government communications, which prevents use of commercial operators
Possible scenarios identified	Not applicable
Any other relevant information from the report	Questionnaire responses confirm PSS users currently use a mix of dedicated and commercial systems across Europe (TETRA, TETRAPOL, commercial GPRS/3G,satellite, RFID). Emphasis in future is integration i.e. simultaneous voice and video over the same network.

C.7 Results of the TC-RSS WG4 questionnaire

Item	*Description*
Document title	ETSI TR 102 733 and ETSI TR 102 734, Re-configurable radio systems (RSS): System aspects for public safety and user requirements for public safety
Author	ETSI TC TTS WG4
Version	V0.0.12 (November 2009)
Abstract	ETSI technical reports referring to a feasibility study of the system aspects (703) and requirements (704) for re-configurable radio systems (i.e. cognitive technologies etc.) for public safety. It identifies and defines the requirements of RRS to the public safety domain, incorporating the results of a questionnaire distributed by ETSI TC RRS WG4 to end-users across Europe. The scope refers to re-configurable radio systems only, and does not define requirements/system requirements for a complete radio replacement system for public safety users.
Requirements or needs identified in report	Defines the role of different public safety authorities, e.g.: • Law enforcement – patrolling to identify and intervene in cases of offence to criminal law, criminal investigation, customs verification, law enforcement in the transportation domain (air, road, rail, sea), custody and transportation of criminal convicts • Emergency medical and health service – provide critical and supportive care of sick and injured citizens and the ability to transfer citizens in a safe and controlled environment. Information required by EMS providers includes patient information, medical information, resource information, incident information and geographical information • Border security (including coast guards) – verification of illegal immigration, verification of the introduction of illegal substances, verification of introduction of goods in offence to customs regulations • Fire-fighting – including fire fighting, search and rescue, management of hazardous materials, protecting the environment, salvage and damage control • Protection of the environment (forests etc.) – typically employing sensor devices • Search and rescue • Crisis management – typically requiring situational information/situational awareness. Requirements defined as: joint operations between different PSS users, ability to operate in unpredictable conditions, ability to communicate when networks are unavailable (i.e. direct mode), terminals interoperability, limited budgets, security of various levels, resilient networks, resource management (i.e. support dynamic prioritisation of available capacity) and scalable networks From the user survey (RRS WG4 questionnaire), the following requirements are identified: • Broadband connectivity • Interoperability between different PS users • Avoid need to use multiple terminals • Communications in tunnels/underground/indoors • Increased capacity, coverage, grade of service, voice quality, robustness

	to interference, reduced call set up time. • Messages of large sizes, access to databases, access to web, video, video conferencing, distribution of images and buildings plans, medical information, bio metric data, weather/traffic information, software updates to terminals in real time.
Possible applications identified in report	1. *Verification of biometric data*. Public Safety officers may check the biometric data of potential criminals (i.e. fingerprints facial/iris recognition) during their patrolling duty. The biometric data could be transmitted in real-time to the headquarters or a center with the biometric archives and the response could be sent back to the Public Safety officers. This would be a positive method of identification during field interrogation stops. 2. *Wireless video surveillance and remote monitoring*. In these types of applications, a sensor (fixed or mobile) can record and distribute data in video-streaming format, which is then collected and distributed to public safety responders and command & control centers. 3. *Automatic number plate recognition where a camera captures license plates and transmits the image to headquarters* or a center with the plate data to verify that the vehicles have not been stolen or the owner is a crime offender. 4. *Documents scan*. In patrolling or border security operations, public safety officers can verify a document like a driving license in a more efficient way. Documents scan is also useful in border security operations where people, who cross the borders, may have documents in bad condition or falsified. 5. *Database checks*. This application area includes all the activities where public safety officers must retrieve data from the headquarters to support their work. 6. *Location/Tracking for Automatic Vehicle/Officer Location*. The public safety officer has a GNSS position localizer on the handheld terminal or the vehicular terminal. The positions are sent periodically to the headquarters so that the command centre can organized and execute the operations in a more efficient way. *7. Transmission of Building/Floor plans and Chemical data*. In case of an emergency crisis or a natural disaster, Public Safety responders may have the need to access the layout of the buildings where people may be trapped or where dangerous chemicals are kept. Chemical data, building or floor plans can be requested to the headquarters and transmitted to the public safety responders. *8. Monitoring of Public Safety officers*. Vital signs of Public Safety officers could be monitored in real-time to verify their health conditions. This is particularly important for firefighters at fire incidents and officers involved in search and rescue operations. *9. Remote emergency medical service*. Through transmission of video and data, medical personnel may intervene or support the team in the field for an emergency patient. *10. Sensor networks*. Sensors networks could be deployed in a specific area and transmit images (thermal) or data to the Public Safety responders operating in the area or to the command centre at the headquarters.
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	PSS requirements capture routine operations, emergency crisis, major planned events, natural disasters and search and rescue – all of which require ubiquitous communications, and the ability to concentrate capacity in incident areas, which commercial networks do not provide. Lack of network

	capacity is mentioned as a key problem during emergency incidents. The document also cites the following reasons (these relate to why PSS requires re-configurable radio systems in addition to voice/data wide area networks to overcome the limitations of existing public safety communications systems in large incident situations, but some are also valid reasons against use of commercial networks): The locations where emergency and disaster relief operations occur are unpredictable and the availability of communications facilities is not guaranteed in the incident area. Even if wireless communications infrastructure exists in the incident area, the first responders may not have the appropriate terminals. Public safety responders need wide area coverage, e.g., in the event of natural disasters like earthquakes or flooding, where a large area may be affected. Support for wide area coverage and higher transmission output is a conflicting requirement with low power consumption and extended battery life for handheld terminals. Public safety organizations must operate in uncertain conditions and difficult environments both from a physical as well as from a radio propagation point of view, due to the presence of radio interferences or obstacles (man-made or natural). Public safety responders have special requirements regarding reliability, responsiveness and security of their communication systems.
Possible scenarios identified	Refers to four scenarios contained in SAFECOM document from US communications programme of the Department of Homeland Security – Public safety statement on requirements for communications and interoperability: 1. Emergency Medical Services (EMS): Routine Patient Services and Car Crash Scenario. A voice conference call is set up between the ambulance and the hospital, while the vehicle's geo-location as well as the vital measurements and treatments of the patient are recorded and transmitted wirelessly. 2. A residential fire scenario: as in the first scenario, geo-location and vital measurements of multiple victims, first responders and vehicles is wirelessly transmitted; additionally, GIS information on building plans, fire hydrant locations, etc is accessible. 3. A traffic stop scenario: the situation message, the police vehicle's ID and geo-location are transmitted; the suspect car's license plate is read and sent to dispatch, where it's queried against several law enforcement databases, and the results are sent back to the police officer; a video stream of the action is available on demand to dispatch; the officer decides to request backup, the nearest vehicle is located by the backup system and the request is forwarded; when the suspect is arrested, information about the crime, the police officer, etc is loaded onto the RFID embedded in the handcuffs; after the arrest, biometric data from the suspect is sent to dispatch, queried against databases, and the answers are sent back; the officer communicates with the tow truck company; evidence and other information is transmitted to the sheriff's office; the case report is sent electronically to the officer's supervisor. 4. An explosion scenario: here the communications analysis is from the incident commander's point-of-view, while all the first-responder requirements described in the previous scenarios are still considered valid; the various (diverse) units that arrive on the scene form an ad-hoc overlay network and provide information about their location and status; GIS information is available on demand to the commanders; distributed sensors

	on the first-responders relay their readings to central command; a secondary perimeter is set up, and a reverse 911 call is sent to fixed and mobile users (civilian) inside the perimeter to evacuate or find shelter; at the same time, the Department of Transportation is notified to divert traffic from the area; critical infrastructure (gas, electricity) is shut down; the commander decides the explosion is not an accident, and directs field agents to treat it as a crime scene, while calling in detectives to investigate; the number of casualties is assessed too high for local hospitals, so coordination with other medical centers is necessary; at the end of the incident all-but-one of each type of team is released.
Any other relevant information from the report	The two ETSI TR refer to various other documents upon which requirements have been based: ETSI TS 102 181 (EMTEL) requirements for communication between authorities/organisations during emergencies TS70.001 – Service specification group services and applications Project MESA: Service specification group statement of requirements SAFECOM, Department of Homeland Security – public safety statement of requirements for communications and interoperability ETSI TR 102 182 – requirements for communications from authorities during emergencies Project OASIS – European disaster and emergency management system WIDENS (wireless deployable network system) – supported by EC IST Framework programme 6. Builds upon MESA statement of requirements.

C.8 Results from the expert group on police cooperation

Item	*Description*
Document title	Draft Council Recommendation on improving radio communication between operational units in border areas
Author	Council of the European Union
Publication date	20 May 2009
Abstract	The paper discusses recommendations on improving radio communications in border areas and more effective cross-border cooperation including interoperable radio communication systems in border areas and between operational services from different Member States. Difficulties in the use of radio communications in border areas are caused mainly by the lack of interoperable interfaces between current systems, which prohibit effective roaming; needs to be addressed. Therefore, significant improvement in voice and low-speed data interoperable capability could be achieved by interconnecting systems where possible. In the long term, law-enforcement and public-safety radio communication systems will need to support and to be able to exchange high-speed mobile data information. However, current law enforcement, public-safety and public networks may not be able to support this. The document recommends that: • Intersystem interfaces be developed and encourages the European Commission to provide funding for them • CEPT / ECC be tasked to study the possibility of obtaining sufficient additional frequency allocation below 1GHz for the development of future law-enforcement and public-safety voice and high-speed data networks; • European standardisation bodies be invited to start producing a European standard satisfying law-enforcement and public-safety services' operational requirements regarding high-speed data communication and roaming functionality in the medium term • In the long term, after the life cycle of current TETRA and TETRAPOL systems has ended, voice and all data functionalities (high and low speed) be integrated in a tightly integrated solution that provides a migration path including interoperability from existing law enforcement and public-safety systems to the new solution • Member States allocate additional frequencies at national level in a coordinated timeframe in cooperation with CEPT • Member States adopt any appropriate local measures in the short and medium term to improve cross-border cooperation.
Requirements or needs identified in report	• A common network standard or standards operating in harmonised frequencies to facilitate fully interoperable communications; • Taking into account investments in existing systems, significant improvement in interoperability in border areas can be achieved as follows: ▪ in the short term, countries with common borders can work together to improve communications with local solutions; ▪ in the medium term, current law-enforcement and public-safety mobile communications systems need to be connected to provide a more effective solution for cross-border communications and facilitate roaming; ▪ in the longer term, a solution for mobile broadband data is required.

	A common standard operating in a harmonised frequency band will make this possible • existing frequency allocations for law-enforcement and public-safety networks may not be sufficient for the development of dedicated infrastructures satisfying operational requirements for high-speed data communication; • there may be opportunities below 1 GHz. to acquire new harmonised spectrum; • in discussing possible additional frequencies, account should be taken of the investments in current networks and also of the increased overall demand for radio spectrum and the fact that it is a scarce resource.
Possible applications identified in report	Not applicable
Possible benefits identified in report	Improve cross border cooperation between operational services
Can the benefits be realised using commercial networks	This was not discussed in length but did mention that current public networks may not be able to support and enable high-speed mobile data information exchange.
Possible scenarios identified	Not applicable
Any other relevant information from the report	Not applicable

C.9 Project MESA

Item	*Description*
Document title	Project MESA; Service Specification Group – Services and Applications; Statement of Requirements (SoR)
Author	MESA
Version	MESA TS 70.001 V3.3.1 (March 2008)
Abstract	Public Safety Partnership Project (PSPP) produced this Technical Specification (TS) during the course of Project MESA (Mobility for Emergency and Safety Applications). It describes the services and applications, which a future advanced wireless telecommunications system should be able to support in order to realize the most effective operational environment for the Sector. Emphasis has been placed on those applications, which current applied technology cannot carry out to the full, but which have been identified by the users and their agencies to be key requirements and capabilities, providing a profile of the common operational and functional requirements of next-generation aeronautical and terrestrial-based, mobile and fixed systems. The document reflects the requirements of public service and public safety agencies to have priority service and system restoration, extremely reliable service, and ubiquitous coverage within a user's defined service area. The document is intended to be a unique source of information in the aim of understanding the often very difficult and dangerous working environments, which the user community is facing, such that Industry can provide the most effective and accurate technical solutions. It establishes an understanding that the advanced needs of the PPDR Sector should be based on a high-mobility, broadband wireless network or related capabilities that allow for the provision of dynamic bandwidth, offering of self healing characteristics and secure network access. Project MESA SoR also reflects the vision of a mobile broadband-shared network that can be simultaneously accessed by multiple users, with multiple applications in a specified geographical area fully independent from availability of public networks and supply of electrical power.
Requirements or needs identified in report	These include but not limited to: • Improvements in spectrum efficiencies. • Incorporation of frequency neutrality and/or agility. • Life-cycle procurements. • Security requirements. • Economical and ergonomically friendly design. • Digital migration in place. • Consistency with existing standards. • Compatibility with multiple international standards. • Two-way communication. • Multiple levels of security. • Multiple levels of availability of service. • End-to-end network integrity. • High-speed, error-free service. • System and network access. • Compliance with the need of the participating nations.

Possible applications identified in report	*Wireless data requirements* include such uses as mobile computing terminal applications, geographic position and automatic location data, emergency signals, transmission of reports, electronic messaging, home incarceration monitoring, and perimeter and vehicle alarms. *Multimedia systems* employing both photographic and fingerprint transmission in conjunction with report automation. *Remotely controlled radio devices* are routinely used for turning on and off surveillance microphones, activating kill switches in vehicles, arming and disarming alarm and monitoring systems, and aiming video cameras. This control can be a one-time data burst or can be a continuous data stream. *Unattended electronic sensors/monitors*, for border surveillance, parolee monitoring and other remote-sensing technologies. *Global location services* for vehicle and personnel tracking, security, and inventory control *Institutional monitoring* such as remote electronic monitoring devise for house arrests and *environmental monitoring* such as real time monitoring of public resources, such as water flow and quality *Telemetry systems* may also provide both an inventory of remaining infrastructure and the control of moving fixed assets, such as fire trucks, snow ploughs, police cars, ambulances, and many other types of equipment used in emergency response, including changeable signs and traveller information radio systems, as well as weather and road condition data transfer from remote sites. *Personal location device* to track the location of an assigned individual for general management purposes and in the event of an emergency. Transmission of forms and reports to central sites from mobile and remote locations. This capability will be used to transmit long data streams to and from central locations and the field in just a few seconds. Video capabilities (real-time and close to real-time) including traffic surveillance, disaster relief, emergency medical services video, point-to-point and broadcast, transmission of videos from field operatives to command and control as well as the other way. Robotic devices for hazardous material and explosive disposal, which require full-motion video that can be transmitted over a short distance (up to 1000 meters), from the control device to the robotic devices. This application may require the use of equipment and technologies developed for explosive atmospheric conditions and/or that will not initiate the explosive device being rendered safe. Lifeguard/water safety personnel often require the support of robotic devices in underwater search and rescue operations, especially when persons, planes, and ships are submerged in water depths greater than 200 feet.
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	The Project MESA SoR reflects the need for a network that is fully independent from availability of public networks and supply of electrical power that satisfies the following requirements: • Transparent and seamless wide-area network applications. • Include multiple levels of security and data encryption schemes that may be a function of the network or a function of the application or communication device to ensure end-to-end data protection. • Offer robust operational management and control systems capabilities.

	• Reflect the requirements of MESA users to have priority operational services and priority system restoration. • An extremely reliable service model and ubiquitous coverage within a user's defined service area.
Possible scenarios identified	Describes a number of details scenarios in pages 40-43 of the document: • Law enforcement – Court house murder • Law enforcement – U.S. State and Urban Police Response to Earthquake Damage.
Any other relevant information from the report	The document includes a detailed statement of specific/unique requirements for the different government and emergency services organisations, giving examples of application needs - some of which are typically not supported in commercial terminals, which supports the argument about the requirement for dedicated networks (and associated terminals).

C.10 Toia Report on Digital Dividend

Item	*Description*
Document title	Extract: Toia Report on Digital Dividend/2008-09-26 - Text adopted
Author	Rapporteur - Patrizia Toia
Version	24 September 2008
Abstract	European Parliament resolution of 24 September 2008 on reaping the full benefits of the digital dividend in Europe: a common approach to the use of the spectrum released by the digital switchover (2008/2099(INI)).
Requirements or needs identified in report	Confirms the societal value of public safety services and the need to include support for their operational requirements in the spectrum arrangements arising from the reorganisation of the UHF band resulting from the switch-off of analogue services. Considers that the part of the harmonised spectrum at Community level dedicated to emergency services should be capable of providing access to future broadband technologies for the retrieval and transmission of information needed for the protection of human life through a more efficient response on the part of the emergency services.
Possible applications identified in report	Not applicable
Possible benefits identified in report	Societal value
Can the benefits be realised using commercial networks	Not applicable
Possible scenarios identified	Not applicable
Any other relevant information from the report	• Recognises that the increased spectrum efficiency of digital terrestrial television should allow for around 100 MHz of digital dividend to be re-allocated to mobile broadband and other services (such as public safety services, radio-frequency identification and road safety applications) whilst ensuring that broadcasting services can continue to flourish • Acknowledges that coordination at EU level would encourage development, boost the digital economy and allow all citizens affordable and equal access to the information society • Calls on the Members States, whilst fully respecting their sovereignty in this regard, to analyse the impact of the digital switchover on the spectrum used in the past for military purposes, and, if appropriate, to reallocate part of that specific digital dividend to new civilian applications • Emphasises the contribution that the digital dividend can make to the provision of enhanced interoperable social services, such as e-government, e-health, e-vocational training and e-education to citizens, in particular those living in less favoured or isolated areas, such as rural and less developed areas and islands • Encourages Member States to consider, in the context of allocating white space, the need for unlicensed open access to spectrum for non-commercial and educational service providers and local communities with a public service mission • Emphasises that Member States may consider technology-neutral auctions for the purpose of allocating frequencies that are liberated because of the digital dividend and making those frequencies tradable; considers, however, that this procedure should be in full compliance with ITU radio regulations, national frequency planning and national policy

	objectives in order to avoid harmful interference between services provided; warns of spectrum fragmentation which leads to the sub optimal use of scarce resources; calls on the Commission to ensure that a future coordinated spectrum plan will not create new barriers to future innovation • In order to achieve a more efficient use of spectrum and to facilitate the emergence of innovative and successful national, cross-border and pan-European services, supports a coordinated approach at Community level, based on different clusters of the UHF spectrum for uni-directional and bi-directional services, taking into account the potential for harmful interference arising from the co-existence of different types of networks in the same band, the outcomes of the ITU Geneva RRC 06 and WRC 07 and the existing authorisations.

C.11 WIK Study

Item	*Description*
Document title	Safety first – Reinvesting the digital dividend in safeguarding citizens (WIK_white paper_full_final)
Author	WIK Consult
Version	Bad Honnef, 5 May 2008
Abstract	Report produced by WIK and Aegis Systems with input from selected public safety organisations, regulators and TETRA vendors. The report recommends that public safety users require dedicated networks because of the unique technical and operational requirements associated with providing mission critical communications, which are extensive coverage (e.g. excess of 99% geographic coverage), capacity (e.g. public safety networks have to be capable of nationwide call set up with latencies of less than 0.5 seconds), reliability (99.999%) and redundancy (e.g. 1+1 or 1+n redundancy, power supply redundancy is essential, etc.). The report goes on to suggest that sub-1 GHz spectrum is required for public safety networks in order to meet their technical and operational requirements. Suggests that there is a 'moral obligation' to assign spectrum to public safety since PSS services are indispensable. Since emergency response ranges from routine to extreme, might be possible to use some novel spectrum allocation methods e.g. pre-emptive spectrum assignment, to provide a 'core' band for PSS use and additional spectrum that can be used when required – but when not required, can be used for commercial systems. Possible for commercial users to share a PSS networks, but not vice versa (other than for non-mission critical applications) due to the cost, complexity and risks associated with upgrading a commercial network to achieve the ubiquitous coverage, reliability, redundancy and capacity that PSS networks require.
Requirements or needs identified in report	Mission critical applications have unique technical and operational requirements, which are not met by commercial networks, since the latter are optimised for financial return on investment. They require dedicated spectrum and control of their own networks because of the flexibility it affords and ability to meet their own specific requirements of security, robustness, immediacy of communications. Public safety users have different requirements with respect to user terminals compared to commercial users – typically public safety terminals need to be designed for use and support for 5-6 years (as opposed to 1-2 for commercial handsets), due to budgetary considerations, training requirements and reliability. All handsets must have the same user interface and all operate in the same way. Mission critical refers to information that must be transmitted because it is crucial to the successful resolution of the emergency operation, requiring: coverage everywhere, instant access to resources, fixed and deployable networks, ability to support mixed traffic, flexibility, security, resilience, and additional network operation e.g. peer to peer/DMO (terminal to terminal communications without connection via the infrastructure).
Possible applications identified in report	• Remote checking of information such as passports and biometric details • Sending detailed photographic images of children lost or people wanted to officers in the field, so they can act on requests immediately • Providing access to Fire Service 'Gazetteer' which is document containing information on which hazardous materials might be kept in particular premises

	• Transmission of live video information from an incident to central command and control, so they have access to the same images as those in the field (and thereby improve decision making) • Relaying ad-hoc video and surveillance camera real time information to patrol cars responding to incidents • Sending of full data on a patients condition from the ambulance to the hospital • Video streaming (e.g. CCTV on scene) • Online access to contacts database • Email and internet • Ability to move the back office into the field • Real time evidence collection • Licence plate recognition • Traffic light sensors.
Possible benefits identified in report	• Improved establishment of command and control – public safety agencies are increasingly moving to field command (although command and control rooms will still remain) • Dissemination of timely information (e.g. medical records, details of dangerous substances, maps, pictures and videos) • More timely response e.g. able to act on requests immediately • Better decision making – those in command and control and in the field have access to the same information at the same time • Interoperability - possibly public safety interoperability can be achieved using DMO only • Better mobilisation of teams and people • More frequent updates on emergency situational reports • Better preparation (e.g. informing hospitals of likely numbers of casualties and the sorts of treatment required) • Better incident provision from the incident area • Voice is still the central means of command and control for public safety, but they are increasingly using data applications • Better 'location' information e.g. location of fire fighters and people within a building, real time viewing of building plans, better ability for incident commander to take decisions such as building evacuation (e.g. if building is about to collapse) • Real time structural awareness.
Can the benefits be realised using commercial networks	The two main problems with using commercial networks for safety critical applications are availability and performance. Cost to upgrade a commercial network to provide the operational requirements public safety need in terms of resilience, redundancy, capacity and coverage needs to be borne by public sector since it is not commercially viable. Problems of public safety users relying on a commercial network operator include: risk of commercial operator becoming insolvent, risk of commercial operator imposing unexpected price increases, meeting specific information security requirements etc. Having a dedicated network allows public safety users to have control over QoS, SLAs etc. (possible that operation and maintenance could be outsourced to a private company). Current commercial networks do not provide 0.5 second call set up, nor

	99.999% reliability, nor power supply redundancy.
Possible scenarios identified	The report refers to a case study of the Buncefield fire – the explosion of the UK's fifth largest fuel distribution depot in Hertfordshire. Explosion took place on a Sunday when public networks were not being extensively used and in area of low population density, and so public safety users were able to make use of GSM/GPRS on that occasion – no need to ask for priority access to the network on that occasion. Problems in obtaining good voice clarity across all of the incident area were experienced.
Any other relevant information from the report	Annex D of the report summarises its main arguments and counter arguments.

C.12 PSC Europe response to the digital dividend

Item	*Description*
Document title	PSC Europe response to the digital dividend hearing
Author	PSC Europe
Publication date	11 June 2008
Abstract	It is a summary of the response provided by PSC Europe.
Requirements or needs identified in report	ETSI has been developing a system reference document. That document, in its current form, concludes that 2 times 15 MHz would be a reasonable amount of spectrum for the new services. However, there are other applications that would require more spectrum. This figure has been developed by ETSI and communicated to the CEPT.
Possible applications identified in report	Not applicable
Possible benefits identified in report	Value should be considered as judged by the end user and the value to citizens and society, as the value for society is not merely economic but includes important social benefits, and will place a high value on the prevention of accidents and/or the rapid handling of incidents that do occur. Generated value is something beyond just the economic value. Total value cannot always be quantified in economic units. Economies of scale – with European PS Agencies, we have a market size of only a few million devices. Harmonization will therefore have huge impact on prices and therefore the industry and the tax payers Cross-border cooperation – as demanded under the Schengen Agreement. As many EU Member States have common borders with several other Member States and therefore many operations or emergency interventions in common, cross-border operation is a vital component of emergency service provision now and in the future.
Can the benefits be realised using commercial networks	No, as public safety: • Needs an infrastructure that is independent from the common commercial networks • Needs an optimised design to carry out group calls (voice, video and data multicasting) • Needs quick connections • Needs independence • In practice, the commercial operators do not accept to grant pre-emptive priorities to the PS agencies.
Possible scenarios identified	Not applicable
Any other relevant information from the report	The combination of: • operational cross-border requirements, • economic benefit to governments and the funding taxpayers via volume effect on unit cost and • facilitation of industry business case in this limited volume but high-tech market, form a package with overriding justification that allows the EC to proceed with e.g. specific mandate or other appropriate measures. Both for operational cross-border cooperation reasons and for economic reasons that help both the investing taxpayers and the industry to build reasonable business case, harmonised frequency arrangements for the PS Services would permit the emergency agencies to deploy data services in an economically feasible way.

C.13 EULER End User Requirement

Item	*Description*
Document title	EULER End User Requirements Deliverable 2.3-1
Author	Dimitrios Symeonidis
Version	V0.8 (September 2009)
Abstract	The objective of EULER (European Software Defined radio for wireless in joint security operations) is to answer the operational question of how a major civil international crisis can be rapidly resolved jointly given the various types of radios used by different national emergency services. The end user involvement package is organised around a framework for usage scenarios and requirements and systematic methodology for the harmonisation of needs at the European level. The document summarises the End-user involvement framework definition and lists past projects, where the conclusions are summarised and the methodology for requirements classification, requirements harmonisation and matching of the EULER scope are presented. EULER intends to provide added value in comparison to the past projects by providing a harmonised, classified and prioritised collection of requirements from past projects, which includes: • SeBeCom analysis • Wintsec analysis • Safecom analysis • MESA analysis • Chorist analysis. The scenario presented is that of a Tsunami describing first hours operations capabilities, communication flows priority, organisation network composition and communication link requirements.
Requirements or needs identified in report	• Interaction between users ▪ Real-time exchange of information between several authorized emergency personal • Applications and services ▪ Data to be transported ▪ Network congestion management requirement • Interoperability, adaptability and flexibility • Reliability and information assurance • Robustness • Sustainability • Environmental safety • Security ▪ Authentication ▪ Access control ▪ Confidentiality ▪ Integrity ▪ Availability.
Possible applications identified in report	• Speech – speech quality, point to point duplex communications, direct mode, ambient listening

- Short messages – paging services, status monitoring, location services
  - able to identify the requested authorized emergency agent(s), and then deploy the appropriate technology to contact them
  - Status monitoring may include breathing air tank levels, accountability monitoring, distress buttons and vital signs monitoring.
  - Location services provide real-time information regarding the position of personnel or vehicles to a command point. The network must support three-dimensional geo-location information transmission.
- Access to databases
  - Variety of data applications including email (text messages), imaging, digital mapping / geographical information services, location services, video (real-time), video (slow-scan), remote database access, database replication, personnel monitoring
- File transfers
  - Supports bulk file transfer
- Images
  - Support images and scene photo transfers
- Video
  - Incident area network video communication service supporting full-duplex, peer-to-peer, mission-critical video and allow for late entry.
  - Near real-time video streaming.
- Multimedia conferencing
  - Incident area network highly interactive service transaction data
  - The network must support a signalling protocol that is capable of providing session control for both voice and video applications, as well as instant messaging
- Web
  - The network must support World Wide Web browser-based applications
- Email
  - Especially useful in noisy environments, or for difficult-to understand data, such as a license plate or a passport number
- Telemetry
  - Environmental telemetry e.g. waters flow and quality, providing instant information and a timely warning of severe change in conditions and early warnings.
  - Transmission of user and patient monitoring telemetry e.g. from inside the ambulance to the receiving hospital's emergency room
  - Transmission of geographical location data (Galileo) e.g. useful for tracking the location of field officers
  - Network of sensors, which are embedded into the field officer's terminals, such as temperature or dangerous gas sensors.
- Instant messaging – peer-to-peer
- Paging including voice paging to one or more participants
- Quality of service
- Pre-emption

	▪ Within all speech services there may exist a requirement for prioritisation and pre-emption of calls. ▪ This service shall allow an authorized user to intervene in an ongoing authority-to-authority call. • Priorities • Two-way communications • Multi-point to multi-point communications ▪ Belonging to groups ▪ Dynamic group creation/ deletion/ modification ▪ Dynamic Group Number Assignment ▪ Group members ▪ Talk group ▪ Group communication interoperability ▪ Group contain • Dynamic updating of data fields ▪ support two-way operation to accommodate the implementation of "smart" systems that automatically update data fields being transmitted from authorized and authenticated user devices
Possible benefits identified in report	Future public safety communications will benefit from the use of massive data transmissions to improve the efficiency of disaster recovery operations. An efficient radio spectrum management optimises the spectrum sharing between the different public safety organizations according to their respective and evolving needs. Sophisticated spectrum management algorithms, which can adapt to changes in the radio environment, can help using radio spectrum more efficiently. EULER proposes a system in which each subset is able to dynamically change the operating frequency band and bandwidth, is able to reallocate its use of radio spectrum bands, is aware of the existence of other wireless communications systems transmitting in the incident area, has sensing capabilities, and is able to inform the other subsets of its spectrum usage in its coverage. All of this contributes to provide a wireless system that is more reliable and resistant to interferences.
Can the benefits be realised using commercial networks	Not applicable
Possible scenarios identified	First Hours of international, state and local Public Safety Operations in response to a Tsunami. • Tsunami monitoring systems are positioned at strategic locations. • First hours: until local and mobile command centres are activated and connected to country's Emergency Operations Centres (EOC), which can last some days due to inundation and receding water. • Ground based wire and fibre communications to the outside world are temporarily disrupted. • First link establishment of V-UHF radio communications (air-to-ship, air-to-ground, air-to-air, ground-to-ground (voice, video, data)). • Information flow – search and rescue first operators, situation awareness video supported.
Any other relevant information from the report	Not applicable

C.14 TETRA Association Spectrum Group study

Item	*Description*
Document title	What data services will the future bring – from a TETRA perspective
Author	TETRA Association Spectrum Group
Version	Indicated as “draft” (November 2009)
Abstract	The document discusses the killer application for TETRA being mission critical group calls, and then discusses the feasibility of carrying missing critical group calls, and other public safety data applications, over LTE networks. The conclusion is that LTE is unlikely to be feasible to replace private networks in the short term, because (i) the LTE standard would need to be modified to support true multicasting group call capability (currently group calls via LTE are proposed to be delivered through a set of unicast IP streams, which means each member of the call receives his/her own copy of the voice stream. This can lead to quality problems (due to echo) and capacity issues due to the cell load created through transmission of multiple copies of the same IP stream), and (ii) LTE would also need to be modified to support direct mode (i.e. terminal to terminal calls that do not go via the LTE network) (iii) Emergency Services require a range of terminals (rugged, environmentally sensitive, covert) which commercial vendors do not provide, and so this would require special development (refers to the case where the GSM standard was modified for the railways, however the modifications required to GSM to create GSM-R were sufficiently large that whilst GSM is supported by many vendors, GSM-R is limited to very few, and prices for GSM-R are even higher than for TETRA).
Requirements or needs identified in report	1. Group calls where all users on the call, without substantial network overheads and/or cell capacity issues, receive the same transmission simultaneously. 2. Nationwide coverage, including ‘difficult’ geographies and indoors 3. Layered priorities/pre-emption (i.e. enabling emergency services to have priority access over commercial traffic, and enabling higher ranks of officer pre-emptive access over lower-ranked officers where required) 4. Queued calls, and the ability to configure queuing conditions 5. User prioritisation (e.g. calls cant go ahead until nominated callers join the call) 6. Encryption of different levels (over the air and end to end)
Possible applications identified in report	Mainly refers to existing functionality e.g.: • 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 Also refers to the need for dispatcher terminals
Possible benefits identified	Bespoke, privately run networks for the emergency services can be developed to give the required level of terminal ruggedness, environmental

in report	protection, audio levels, battery life, accessories, and resilience, coverage, availability and security at the network level. These factors make it difficult to reuse networks and terminals taken from the consumer market and to obtain the economies of scale that the consumer market brings.
Can the benefits be realised using commercial networks	Primary reason given is that there is currently no standardisation activity going on at present to adapt LTE to meet emergency services requirements, and if there was to be activity, this would take some time to complete. Also refers to the additional cost to modify commercial networks to deliver emergency services functionality [which *assumes* this cost is higher than the cost to deploy a new, bespoke private network for the emergency services]. Reasons listed in the document: 1. A public network provider will want to invest in coverage where the population, and so where the revenue generation is, with little incentive to invest in areas of low-density population. The cost of network expansion may have to be borne by the public safety community alone. 2. 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 may be the basis for litigation. 3. 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. 4. 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 the public safety community access in these conditions. 5. 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.
Possible scenarios identified	Not applicable
Any other relevant information from the report	Refers to WiMAX being “easier to deploy for a privately owned mission critical user base”, due to network scalability (more flexible bandwidth choices and no need for harmonised paired bands) and less spectrum being needed (i.e. because it uses unpaired spectrum).

C.15 Wireless broadband study by Public Safety Spectrum Trust Chairman

Item	*Description*
Document title	Public Safety Radio Communications; Wireless Broadband is not an alternative to LMR mission critical voice systems
Author	Chief Harlin R. McEwen Chairman, Communications & Technology Committee International Association of Chiefs of Police
Version	Draft (12 October 2009)
Abstract	The paper discusses using wireless broadband for data sharing purposes and the danger of assuming that wireless broadband will offer an alternative to traditional LMR (land mobile radio) mission critical public safety voice systems.
Requirements or needs identified in report	Before LMR systems could be supplanted, broadband services would first need to be deployed to the level that provides the same extensive coverage that mission critical voice systems provide, including in-building coverage in many instances. Because coverage area decreases as data rate increases, covering the same area at the same level of reliability with broadband services will require even more sites than the number used today for voice. If LTE developers were to eventually develop standards for mission critical broadband voice, the public safety community would need to be involved in the equipment development and would need to see it tested and work in the actual public safety environment on a trial basis before they would be convinced it would be reliable enough to use as an alternative to current LMR narrowband voice systems. System operators and users then would need time to procure and deploy appropriate equipment and devices. The reality of broadband coverage build-out, standards and equipment development, testing in the public safety environment, and follow-on procurement means it would likely be 10 to 15 years or more before most public safety entities would be in a position to seriously consider substituting broadband voice for today's LMR mission critical voice solutions. The goal is that a Shared Wireless Broadband Network would give public safety: • Broadband data services (such as text messaging, photos, diagrams, and streaming video) not currently available in most existing public safety land mobile systems • A hardened public safety network with infrastructure built to withstand local natural hazards (tornadoes, hurricanes, earthquakes, floods, etc) that would include strengthened towers and backup power with fuel supplies to withstand long term outages of public power sources • Nationwide roaming and interoperability for local, state, and federal public safety agencies (police, fire and EMS) and other emergency services such as transportation, health care, and utilities • Access to the Public Switched Telephone Network (PSTN) similar to current commercial cellular services • Push-to-talk, one to one and one to many radio capability that would provide a back-up to (but not replace) traditional public safety land mobile mission critical voice systems • Access to satellite services to provide reliable nationwide communications where terrestrial services either do not exist or are temporarily out of service

Possible applications identified in report	Not applicable
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	The fact is there are currently no standards being developed or even planned to provide such a service. The public safety community has endorsed Long Term Evolution (LTE) as the preferred broadband standard for public safety data products and the latest version of that standard (V8) is strictly a data standard that does not include voice capability. The next version (V9) due in late 2010 or early 2011 is planned to include VoIP capabilities but that version will not have any capability to provide one-to-many communications and talk around (unit to unit) voice necessary for mission critical public safety communications. LTE is a commercial standard that does not recognize the mission critical voice communications needs of public safety. That means that if a first responder cannot reach the network (i.e. a police officer in trouble in a building and his radio unit cannot reach a repeater) or there is no network then the unit is useless. That means no communications and a possible life-threatening outcome for the police officer.
Possible scenarios identified	Not applicable
Any other relevant information from the report	On September 11, 1996, PSWAC released a report setting forth the current and future spectrum needs of public safety. Among the findings of the PSWAC report was that 97.5 MHz of new public safety spectrum was needed by 2010, including 25 MHz within five years (i.e., by 2001). In November 2007, the FCC issued the Public Safety Spectrum Trust (PSST) a nationwide Public Safety Broadband License (PSBL) for 12 MHz of spectrum in the upper 700 MHz band (10 MHz of broadband spectrum and 2 MHz of guard band spectrum). The FCC Second Report and Order also directed that the Public Safety Broadband Licensee would negotiate with the commercial operator(s) to set appropriate rules and technical standards to ensure maximum interoperability, reliability, redundancy, competition, innovation and choices for public safety customers using this spectrum. The network would include a satellite-based element to ensure continuous operations when terrestrial/ground-based equipment is knocked out or in areas where there is no terrestrial service. From January 24, 2008 through March 18, 2008, the FCC conducted Auction 73. Almost all of the 700 MHz spectrum, with the exception of the D Block, was sold with the proceeds reaching almost $20 billion. Although there has been a lot of speculation as to why the D Block was not sold, most in public safety believe it was because the industry had its eye on the unencumbered spectrum that did not include any public safety requirements. On March 20, 2008, the FCC issued an order delaying further D Block action until further notice. One issue raised in the Hearing by some Members of Congress were concerns about how much it will cost to build a nationwide public safety broadband network and how it will be funded. Estimates of $10 billion to $40 billion have been floated without any real supporting documentation. There is general agreement that if public safety and the private sector can leverage existing private and public infrastructure the cost can be significantly reduced. One commercial company has said that if existing commercial infrastructure was used their cost estimate would be about $13 billion. Eventual total cost of the network will also be influenced by local build-out decisions. Some commercial companies who have indicated their interest and support for a nationwide public/private network have said it is feasible to fund a nationwide public/private network through the public/private partnerships envisioned. This appears to be the only current option unless Congress were to fund the build out.

C.16 Hansard Report

Item	*Description*
Document title	Lords Hansard text (debate on the second reading of the Digital Economy Bill) – document reference XEMS1002 – Lords Hansard text
Author	www.parliament.uk (transcript of debate)
Publication date	2 December 2009
Abstract	During the second reading of the Digital Economy Bill, Lord Lucas raised a proposed amendment relating to reserving spectrum for the Emergency Services, suggesting that 15 MHz of spectrum within the band 'allocated by the EU' (referring to spectrum below 1 GHz, and digital dividend spectrum specifically, which is discussed in Council recommendation 10141/09). The amendment asks Ofcom to consider reserving spectrum for Emergency Services use.
Requirements or needs identified in report	"We will want our emergency services to have a really modern and effective system that is equivalent to the iPhone".
Possible applications identified in report	Not applicable
Possible benefits identified in report	1. Many of the companies who produce TETRA equipment are based in the UK and therefore the UK export market has benefited from the harmonised development of the TETRA standard 2. Vital for national security reasons
Can the benefits be realised using commercial networks	Not applicable
Possible scenarios identified	Not applicable
Any other relevant information from the report	Not applicable

C.17 Safecom document

Item	*Description*
Document title	Department of Homeland Security, Public Safety Statement of Requirements for Communications and Interoperability (including annex on SAFECOM summit)
Author	US Department of Homeland Security Office for Interoperability and Compatibility (OIC)
Publication date	Volume II Version 1.2 (August 2008)
Abstract	Document contains the assembled requirements for system of interoperable public safety communications across all local and national 'first responder' emergency services communications systems. Describes the public safety environment and the types of applications that might be expected to be used in the future. Two volumes exist – volume 1 is a qualitative description of the types of application that might be required, and volume is quantitative (i.e. in terms of specific network performance requirements and metrics).
Requirements or needs identified in report	Requirements include: • Different hierarchies of users and system • Different modes of communication (with/without a network) • The need for security in communications and in information • Support for command and control processes (i.e. mobilisation of teams, prioritisation of communication, decision making) • Describes a 'system of systems' incorporating all public safety communications modal requirements from wide area networks through to local networks, incident-specific networks and personal area networks (e.g. representing the set of devices that an individual public safety officer users) • Ground based and aerial pictures taken at the scene of an incident, to inform follow on action (e.g. alert hospitals to numbers and types of casualty) • Telemedicine techniques require high quality video images to enable viewing of things like patient's burns or skin/bone details • Emergency button for high-priority treatment of emergency calls • Need to establish connection with a large number of users • Ability to restrict access to information to selected individuals.
Possible applications identified in report	Includes a detailed list of different voice, messaging, data, image and video applications for each of police, fire and ambulance services, including who the communication occurs with, for what purpose and with what special constraints. Examples: • Personal area networks e.g. if a bullet-proof vest detects an impact or a fire-fighters helmet is impacted, it can originate a message to the appropriate person • Full duplex, peer to peer and mission critical voice applications • Peer to peer instant messaging • Automated database updating • Bulk file downloads/uploads • Email/internet

	• Biometric identification techniques • Voice language translation.
Possible benefits identified in report	Diagnosis and treatment in routine health cases for remote/rural communities e.g. remote doctor's viewing of a patient.
Can the benefits be realised using commercial networks	Special constraints include: • High priority calls that need to be secured to protect privacy and maintain chain-of-command authority • Very high resolution video pictures • High priority images requiring rapid transportation between different officers • Voice communications needed to authenticate and authorise personnel to follow specific courses of action • Requirement to be able to communicate when local infrastructure may not be operational (e.g. due to a major incident).
Possible scenarios identified	Describes a number of details scenarios in pages 14-18 of the document: • EMS – routine patient services and car crash scenario • Fire – residential fire scenario • Law enforcement – traffic stop scenario • Multi service – explosion, hurricane, earthquake.
Any other relevant information from the report	The document includes a detailed statement of functional requirements for device/terminal features for police, fire and ambulance users, e.g. interfaces, storage requirements - some of which are typically not supported in commercial terminals, which supports the argument about the requirement for dedicated networks (and associated terminals).

C.18 Westminster e-Forum

Item	*Description*
Document title	Westminster eForum keynote seminar, Emergency Services and Public Safety Spectrum
Author	Westminster eForum (transcript of event)
Publication date	11 June 2009
Abstract	The document describes proceedings at the Westminster eForum keynote seminar on public safety spectrum held during June 2009.
Requirements or needs identified in report	Discusses the different functional requirements that the Emergency Services have: • Complete resilience • Pre-emption functionality • Coverage • Confidentiality • Confidence (that a connection can be made immediately) • Operation in remote and extreme conditions.
Possible applications identified in report	Possible need for a portfolio of technologies including sensing devices etc. Requirements for “all functionality in one device” Emergency button functionality important Talk groups/dispatch More data/faster data Transfer of images and pictures.
Possible benefits identified in report	Not applicable
Can the benefits be realised using commercial networks	Commercial networks not designed for resilient communications (comment from Ericsson: can resilience not be provided through emergency services having access to all five mobile networks, rather than just the one? Also, pre-emption functionality is built into 3GPP standards, it is just not fully implemented at present).
Possible scenarios identified	Not applicable
Any other relevant information from the report	Discussion about different spectrum alternatives and digital dividend spectrum. Martin Cave gave presentation on evaluating alternatives – suggesting there is a “substitution margin” between using dedicated networks and using general (commercial) networks, that should be evaluated.

C.19 PSC Europe White Paper

Item	*Description*
Document title	Public Safety First
Author	Jeppe Jepsen
Version	-
Abstract	This white paper discusses the need for spectrum for Public Safety Services (PSS), through the reallocation of Digital Dividend spectrum, putting forward arguments for further dedicated spectrum for mission critical communications and provides a view of the technical and usage characteristics of next generation PSS radio systems.
Requirements or needs identified in report	Need to be able to gain access to a wireless service to increase efficiency, make it easier to share information, reduce costs, while on the move, and using networks, which are secure, reliable, resilient and available across a wide geographic area regardless of population density. The need for ubiquitous coverage and spectrum between current PSS allocations (around 380MHz and 862MHz) is essential. PSS mission critical broadband communications will empower PSS organizations to move human resources into field, increasing situational awareness and facilitating command and control. Broadband communications will be used to collect and disseminate timely information such as medical records, details of dangerous substances, maps, pictures and video to the various emergency responders. Broadband communications can, for example, support Most mission critical operations depend on voice communications and currently have only two 5 MHz-wide blocks available in the harmonised spectrum. There are already problems with supporting voice traffic at major incidents and planned events. The integrated broadband data services, which are emerging for PSS organizations, require more bandwidth - ideally two paired 15 MHz-wide blocks – 15 MHz. for day to-day use and additional 15 for major incidents. PSS organisations require this dedicated spectrum and their own networks because of the flexibility it affords – the ability to meet their own specific requirements so that they can maximise the advantages provided by broadband services. Dedicated networks employing a dedicated spectrum band are widely used today because it is considered the best way to provide secure, robust and immediate communications for PSS radio systems. The spectrum released can provide access to spectrum in the amounts and within the timescales needed by PSS organizations. PSS organisations require their own spectrum to deploy whatever technologies can meet their service and application needs in an appropriately designed network to meet their operational requirements. Also important when identifying spectrum to take into account other considerations including a sufficient size market for the development of equipment by vendors and the cost of ownership of networks required to support the services and the match against future budgets such as economies of scale and potential for inter-operability.
Possible applications identified in report	These include: • remote checking of information such as passport and biometric details • the sending of detailed photographic images of children lost or people

	wanted to officers out in the field so they can act on requests immediately • providing access to the Fire services Gazetteer – a document containing information on what hazardous materials might be kept on a premises • transmission of live video information to the central command and control personnel so they can have access to the same visual information as their personnel in the field • relaying of ad-hoc video and surveillance camera real time information to patrol cars responding to incidents; or • sending of full data on a patient's condition from the ambulance to the hospital.
Possible benefits identified in report	Societal welfare – to protect life, welfare, and property.
Can the benefits be realised using commercial networks	Possibly some services offered by commercial networks are suitable for certain public safety applications. However, because the mission for PSS organisations necessitates specific requirements for robust mission critical communications in terms of access, redundancy and quality of service, these demands are not suited for commercial networks.
Possible scenarios identified	Not applicable
Any other relevant information from the report	There is a significant risk that basing the award of spectrum on price or average utilization will fail to provide PSS users with sufficient spectral resources. The utilization rate of public spectrum ranges from near constant (e.g. some radar systems and fixed point to point radio links), to mostly idle (e.g. some emergency communications spectrum). A dedicated network in a dedicated spectrum band allocated and assigned to PSS users is the best way to ensure secure, robust and immediate radio communications.

C.20 Report for BAPCO

Item	*Description*
Document title	The “Business Case” for Blue Light Spectrum
Author	David Happy
Publication date	26 August 2009
Abstract	This document was written for BAPCO to justify the request for dedicated and harmonised spectrum for blue light services. It discusses the operational need, current policy, why the current system is not working and why it is not possible to quantify a human life.
Requirements or needs identified in report	Changes in operational needs due to: • Terrorist threats (9/11, July bombings etc.) • Natural disasters (flooding in the UK) • Technical advances of mobile technology • Future events e.g. London 2012 Olympics In a serious accident, the ability for services to inter work seamlessly would improve coordination and lead to markedly improved service levels.
Possible applications identified in report	The ability of a police or fire operative to be able to transmit in real-time images of casualties to local Hospital professionals could assist in preparing the Casualty departments with information and knowledge that would otherwise not be available until the triage process started on arrival at Casualty. Missing person tracing and the ability to use technology to “fit” real-time images of suspects with data already held on them is another way in which the UK could “work smarter.”
Possible benefits identified in report	Safety of life.
Can the benefits be realised using commercial networks	Possibly but there is not enough spectrum for the network to work properly.
Possible scenarios identified	Not applicable
Any other relevant information from the report	In the USA, there is a nation-wide reservation of 97MHz of spectrum following on from a review of spectrum shortage. During 9/11 there were communication problems that could have been prevented and which led to many avoidable deaths amongst fire fighters. During June 2009, The European Council adopted a Recommendation (recommendation 10141/09) setting out the importance of cross border cooperation between police forces. This follows the so-called “Pruem decision” on the stepping up of cross border cooperation, particularly in combating terrorism and cross-border crime. It is widely recognised that in an increasingly interconnected world, more crime will be of a cross border nature – and that this trend will increase. The Council make several critical recommendations as regards next generation spectrum for the use of the blue light services, including (page 4): “the Electronic Communication Committee (CEPT/ECC) be tasked to study the possibility of obtaining sufficient additional frequency allocation below 1GHz for the development of future law-enforcement and public-safety voice and high speed data networks.” And: “that ministries responsible for police and justice be encouraged to contact their counterparts responsible for spectrum policy to ask for their assistance

with the above proposal, given the important role of the national frequency administrations."

The Cave Audit of 2005 at section 8.5 already makes reference to emergency spectrum, and makes clear that the Cabinet Office is responsible where there is an emergency. We have a pandemic now, swine flu, and therefore the circumstances already exist for this provision to be invoked should the blue light services so request.